

一橋大学財務リーダーシップ・プログラム

リスクマネジメントの最近の動向

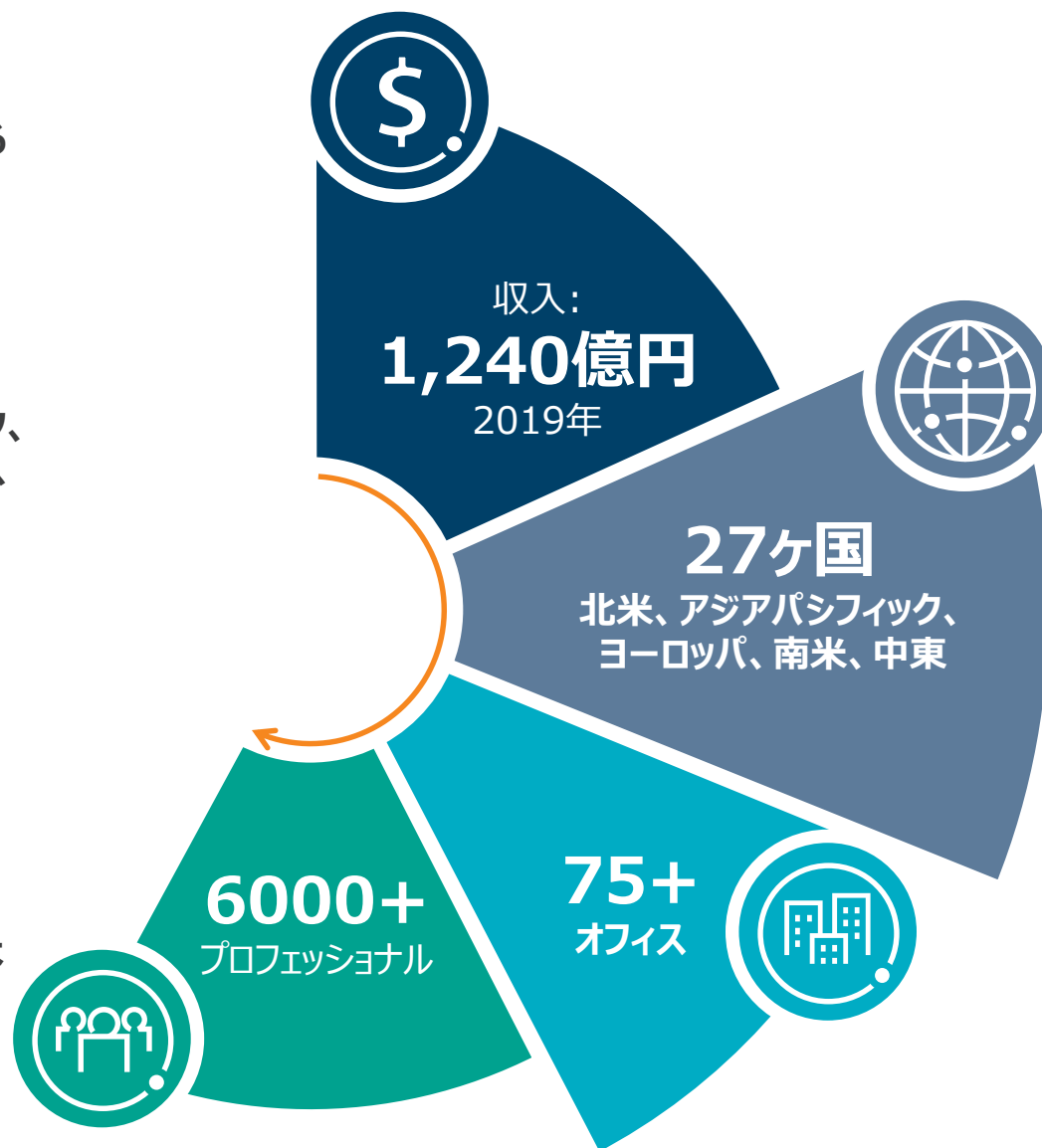
～次世代のリスクマネジメントを目指して

神林 比洋雄
プロティビティLLC 会長
2020年2月14日

講師とプロティビティのご紹介

プロティビティのご紹介

- プロティビティは、企業のリーダーが自信をもって未来に立ち向かうために、高い専門性と客観性ある洞察力や、お客様毎に的確なアプローチを提供し、最善の連携を約束するグローバルコンサルティングファームです。
- 27ヶ国、75を超える拠点で、プロティビティとそのメンバーファームはクライアントに、ガバナンス、リスク、内部監査、経理財務、テクノロジー、オペレーション、データ分析におけるコンサルティングサービスを提供しています。
- プロティビティは、フォーチュン1000の60%、フォーチュングローバル500の35%の企業にサービスを提供し、また、成長著しい中小企業、上場準備企業、政府機関等も支援しています。
- 米国ではプロティビティのマネージングディレクタがCOSOのボードメンバーや、COSOの会長を、日本では会長の神林が日本内部統制研究学会会長を歴任しています。
- プロティビティは、1948年に設立され現在S&P500の一社であるRobert Half International (RHI)の100%子会社です。



プロティビティの海外ネットワーク



The Americas				Europe/Middle East				Asia-Pacific	
1. UNITED STATES Alexandria, VA Atlanta, GA Baltimore, MD Boston, MA Charlotte, NC Chicago, IL Cincinnati, OH Cleveland, OH Dallas, TX Denver, CO Ft. Lauderdale, FL Houston, TX Kansas City, KS	Los Angeles, CA	San Jose, CA	4. CANADA Kitchener-Waterloo Toronto	10. FRANCE Paris	14. UNITED KINGDOM Birmingham Bristol Leeds London Manchester Milton Keynes Swindon	18. QATAR* Doha	23. AUSTRALIA Brisbane Canberra Melbourne Sydney	25. INDIA* Bengaluru Chennai Hyderabad Kolkata Mumbai New Delhi	
	Milwaukee, WI	Seattle, WA	5. CHILE* Santiago	11. GERMANY Frankfurt Munich		19. UNITED ARAB EMIRATES* Abu Dhabi Dubai			
	Minneapolis, MN	Stamford, CT	6. COLOMBIA* Bogota	12. ITALY Milan Rome Turin		20. SAUDI ARABIA* Riyadh	24. CHINA Beijing Hong Kong Shanghai Shenzhen	26. JAPAN Osaka Tokyo	
	Orlando, FL	Tampa, FL	7. MEXICO* Mexico City		15. BAHRAIN* Manama	21. EGYPT* Cairo			
	Philadelphia, PA	Washington, D.C.	2. ARGENTINA* Buenos Aires	8. PERU* Lima	16. KUWAIT* Kuwait City	22. SOUTH AFRICA* Durban Johannesburg			
Phoenix, AZ	Winchester, VA	3. BRAZIL* Rio de Janeiro São Paulo	9. VENEZUELA* Caracas	13. THE NETHERLANDS Amsterdam	17. OMAN* Muscat				
Pittsburgh, PA	Woodbridge, NJ								
Portland, OR									
Richmond, VA									
Sacramento, CA									
Salt Lake City, UT									
San Francisco, CA									

*Protiviti Member Firm



プロティビティLLC 会長兼シニアマネージングディレクタ 神林 比洋雄(かんばやし ひよお)

1976年アーサーアンダーセン入社。国内外を含む監査及びビジネスコンサルティング業務に従事。朝日監査法人（現あずさ監査法人）代表社員、本部理事、および、アンダーセンワールドワイド組織の取締役を歴任。2003年株式会社プロティビティジャパン（現プロティビティLLC）創設と共に代表取締役社長就任、プロティビティ・エグゼクティブ・カウンシルボードメンバーを歴任、16年より現職。

ガバナンス、戦略、ERM、業務改善、ITシステム、内部統制、内部監査に関わるコンサルティングを多数手掛け、グローバル化における組織ガバナンスの在り方、戦略推進を目的としたERMの構築、コンプライアンスやSOX対応等の指揮・監督を行う。

02年外務省改革委員会アドバイザー、05年経済産業省 企業行動開示評価委員会事務局長、08年日本監査役協会コーポレート・ガバナンスに関する有識者懇談会委員。各種業界、企業等における講演など、戦略リスクを中心に、多方面にて攻めと守りのガバナンスを基盤とするERMの高度化を通して日本企業を支援。

多摩大学大学院 客員教授ERM担当（04～09年）、青山学院大学専門職大学院 客員教授ERM担当（10～12年）、早稲田大学大学院商学研究科講師ガバナンス・ERM担当（11～14年）、一橋大学財務リーダーシッププログラム講師（15～）。

日本内部統制研究学会会長（16～19年）。

双日株式会社社外監査役（17～）、株式会社村田製作所社外取締役（18～）。

公認会計士。

■ 講義のテーマ

「リスクマネジメントの最近の動向」

～次世代のリスクマネジメントを目指して

■ 講義の目的

- かつて経験したことのない、経営環境の変化にリスクマネジメントの位置づけが大きく変わろうとしています。欧米では、リスクテイクのためにリスクマネジメントを行い、過度のリスクテイクを回避するためにガバナンスを強化しています。一方、日本では、リスク回避のためにリスクマネジメントを行い、リスクテイクのためにガバナンスを強化しようとしています。
- この真逆の動きになかで、さらなるリスクテイクのために日本企業が検討すべき次世代のリスクマネジメントの在り方について、ガバナンスと内部統制との統合を果たす中で、整理を試みます。

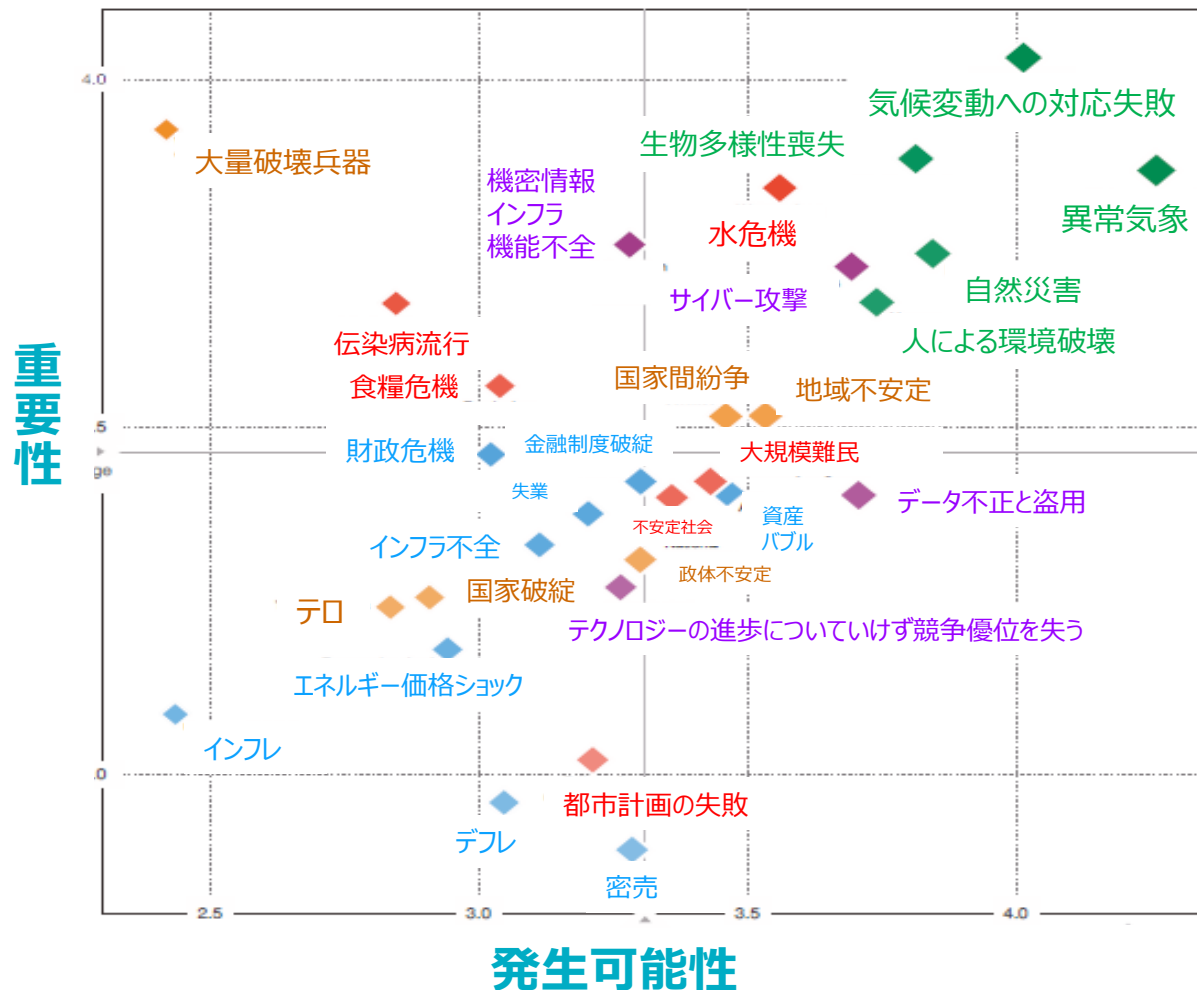
■ アジェンダ

1. 激変する経営環境とリスク～拡大するその定義
 2. 戦略達成のためのリスクマネジメント
仮説指向プランニング
 3. ESG／SDGs リスクへの対応
 4. DXとサイバー・セキュリティリスク
 5. 人材トランスフォーメーション・イノベーションのリスク
 6. リスクと内部統制・ガバナンス
- まとめ

1. 激変する経営環境とリスク ～拡大するその定義

世界はリスクをどう見ているか～「ダボス会議 2020 リスクレポート」より

今後10年の発生可能性と負のインパクトについて、世界経済フォーラム専門家メンバー1,047名へのアンケート調査



- 経済
- 環境
- 地政学的
- 社会
- テクノロジー

ついに気候変動などの
環境が発生可能性の
トップ5を独占
サイバー攻撃などの
テクノロジー、
水危機
などの重要性が増加

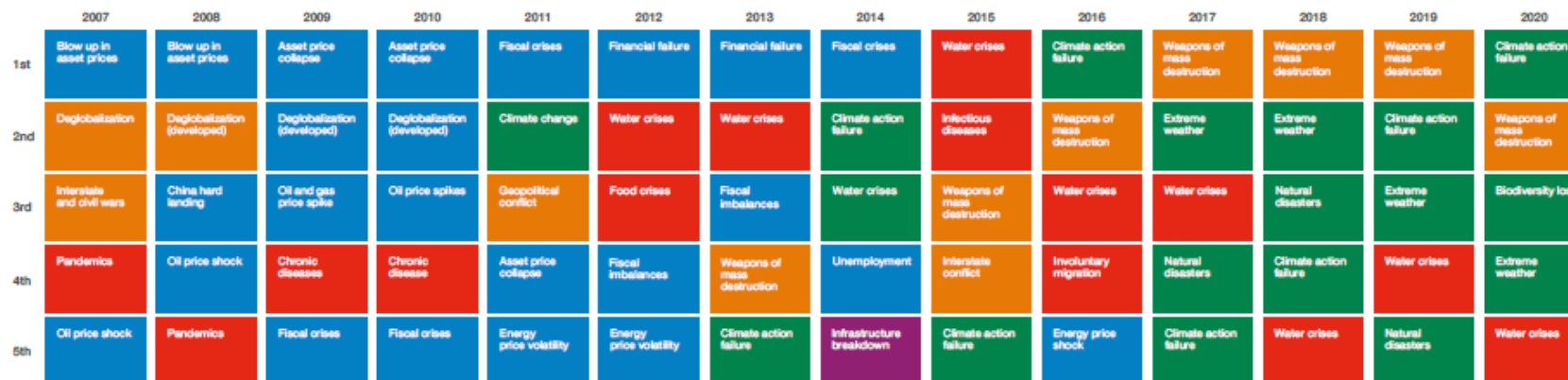
環境リスクがさらに増大

2007年から2020年の14年間のトップ5の重要リスクの変化（2020年ダボス会議より）

発生可能性



影響度



経済

環境

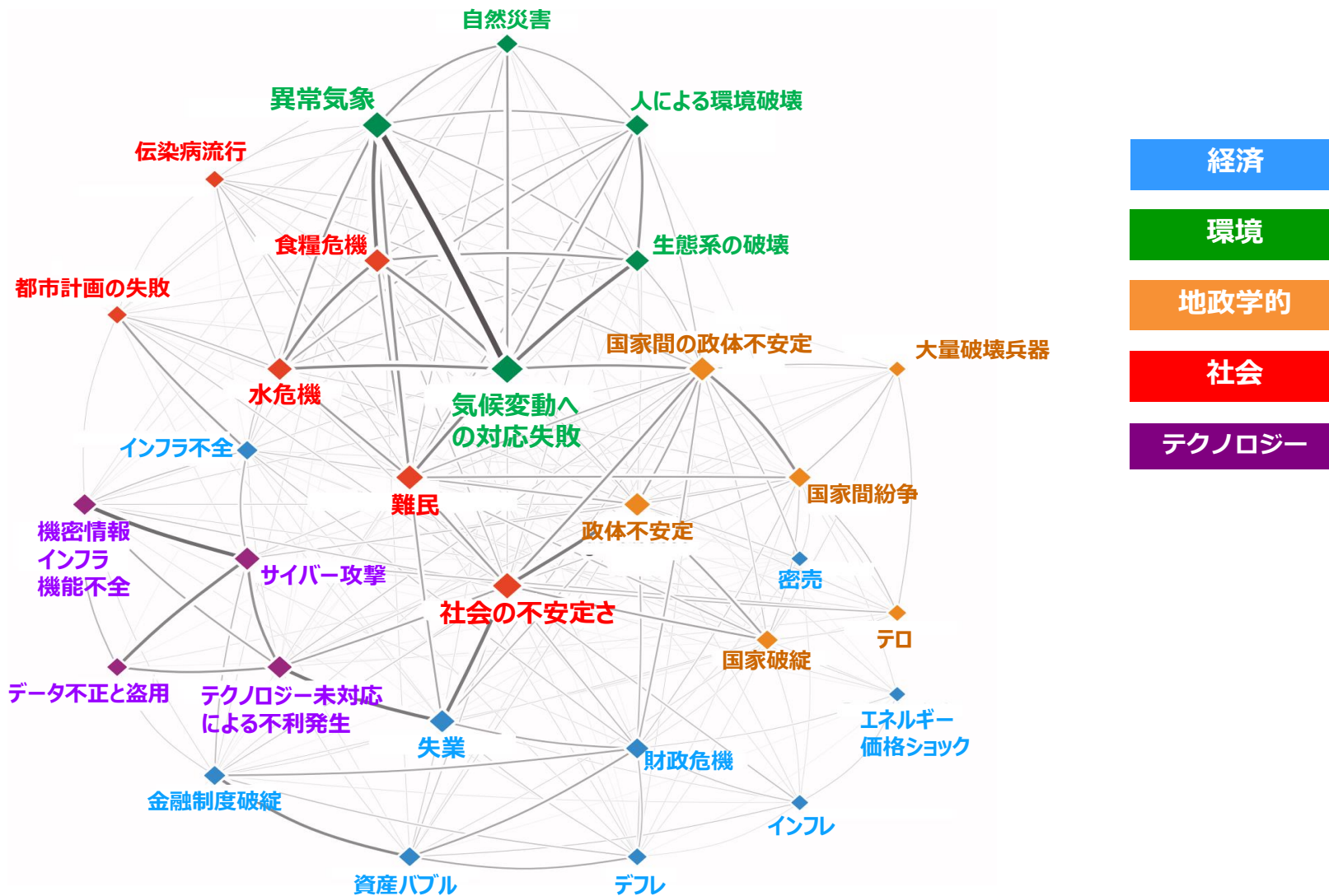
地政学的

社会

テクノロジー

参考：リスクの相互関連・依存 ～2020ダボスリスクレポートより～

リスクシナリオの検討では、相互関連・依存を考慮し、究極のリスク源泉の特定が重要



メガトレンドと巨大リスクにいかに対処するか

メガトレンドが、企業経営に影響を及ぼす巨大リスク

	経済	地政学	環境	社会	テクノロジー
メガ トレンド	<ul style="list-style-type: none"> • 大国による“自国中心主義”化 • 経済力のメガシフト • 中国バブル崩壊リスク • 次の金融危機に対する当局対応不全リスク 	<ul style="list-style-type: none"> • 分断（EU、米国内、米中、日韓）による影響拡大 • 中東での関係国勢力確保競争 • 大量破壊兵器の開発・使用の脅威 	<ul style="list-style-type: none"> • 資源の制約、エネルギー問題深刻化 • 地球受容力の限界 • 温暖化、CO2増加 • 食料不足、農地の減少、水資源の争奪 	<ul style="list-style-type: none"> • 先進国と新興国間の格差縮小と「国内格差」拡大が同時進行 • 人口爆発と人口減少の2極化進行 • 先進国での高齢化 • データ不正情報漏洩 	<ul style="list-style-type: none"> • スマート化の進展 • ナノテクノロジー、医療・ライフサイエンスにおけるイノベーション • CASE • サイバー攻撃の常態化と影響の深刻化
巨大 リスク	<ul style="list-style-type: none"> • 世界的不況の到来 • 大国の保護主義政策により通商リスク拡大 • 資産価値の崩壊リスク • 中国、インド等企業の急速なグローバル化、市場支配地図の変化 	<ul style="list-style-type: none"> • 新オイルショックの勃発 • 軍事衝突がもたらす世界経済への悪影響 	<ul style="list-style-type: none"> • コスト構造の劇的変化（調達、オペレーション） 	<ul style="list-style-type: none"> • 社会や市場の変化に柔軟に対応できない企業の凋落 • 企業ブランド、レピュテーションの毀損 	<ul style="list-style-type: none"> • 現状破壊的ビジネスモデルの出現 • サイバー攻撃による業務への甚大な影響 • 新興国企業による知的財産の盗用と市場参入

* 出所：Protiviti、世界経済フォーラムや、国内のシンクタンク等の公表情報をもとに作成

- **長寿企業を支えてきた日本的良さの見直しー不易流行、何を変え、何を残すか**
- **ガバナンス、ERM、内部統制は、戦略の実現を支える仕組みであることから、今までの、“居心地の良さ”に甘んじることなく、他律的な要請を念頭に置くも、自律的な仕組みとして、再構築の是非の検討を継続することが重要です**

そもそもリスクとは ～発想の転換～

語源：ラテン語のRisicare「勇気をもって試みる、あるいは挑む」

よくあるリスク分類

- (1) **結果系分類**：自然災害などの損害をベースにした、いわゆる怖いもの（保険リスク）
- (2) **成果系分類**：**「報われるリスク」**：投下した経営資源より成果が大きくなるもの
「報われないリスク」：いかに努力しても損失のみが発生するもの
- (3) **源泉系分類**：外部・内部の発生要因からみたリスクの源泉に焦点を当てるもの

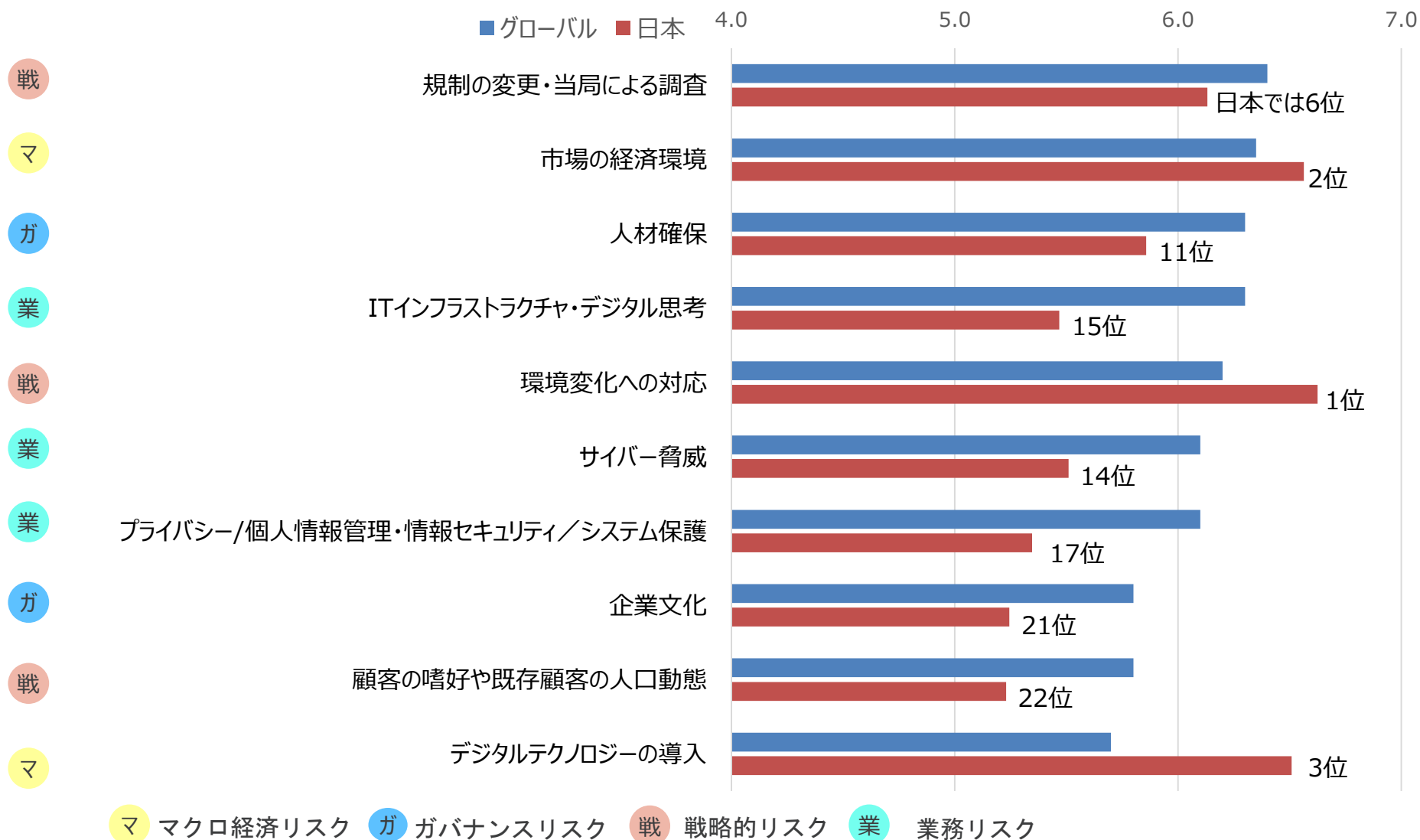
(2) の例：

- 企業買収などは、しっかり対応すればコストを上回る成果が期待できる**「報われるリスク」**
- 会社法の「損失の危険」や、金商法の「財務報告の虚偽記載リスク」は、本来自律的に取り組むべき課題だが、法制化されたことから、“やらされ感”も強く、**「報われないリスク」**
- リスクとは、怖いものでコストドライバーとの“思い込み”に捉われない
- 事業リスクである「報われるリスク」即ち**バリュードライバー**を全社的に管理する仕組が重要

◆ **リスクは変化の可能性**と捉え、**リスクの源泉**に焦点を当て、企業理念を実現すべく策定される戦略の達成可能性の確からしさを高める全社的な工夫が肝要

トップ10リスク（源泉系） グローバルと日本の比較

プロティビティ及びノースカロライナ大学のERMイニシアティブ、並びにプロティビティ
ジャパンが実施したそれぞれ約千名、60名の取締役および経営者へのサーベイより



【33業界全体／FY2018】

FY2018

3,644

社

FY2017

3,600

v.5.0

A 外部環境リスク				
	FY18	FY17	差	
1 競合他社	2704	2659	45	
2 顧客ニーズ	1957	1904	53	
3 技術革新	922	862	60	
4 外部環境への感応度	2962	2906	56	
5 出資者の動向	1196	1137	59	
6 資本調達	1239	1216	23	
7 政体の安定性	1299	1284	15	
8 外交関係	138	100	38	
9 関連法規	3260	3213	47	
10 規格変更	181	169	12	
11 業界特性	527	508	19	
12 地域特性	1902	1880	22	
13 商慣行	207	190	17	
14 金融市場	2984	2972	12	
15 災害・環境的損失	3141	3063	78	
16 気候変動	748	709	39	
17 少子高齢化	674	613	61	
18 サイバー攻撃	1143	1044	99	

B 業務プロセスリスク										
	FY18	FY17	差		FY18	FY17	差		FY18	FY17
(a) 財務				(b) 権限委譲				(d) ガバナンス		
1. 価格				30 リーダーシップ不全				40 組織文化		
19 金利変動	1289	1282	7	31 統制不足	267	231	36	41 CSR	378	346
20 為替変動	2259	2228	31	32 アウトソーシング統制	964	923	41	42 取締役会の実効性	1	1
21 投資持分の価値変動	893	859	34	33 勤務評価基準	246	200	46	43 後継者計画	242	215
22 商品相場変動	229	235	-6	34 変化への順応性	844	828	16	44 グループガバナンス	164	132
23 金融商品変動	820	819	1	35 縦・横の組織内コミュニケーション	163	144	19	(e) 評判		
2. 流動性				(c) 情報処理/IT				45 コーポレートブランド	1766	1706
24 資金不足	730	698	32	36 データの完全性	18	17	1	46 投資家とのエンゲージメント	20	20
25 機会損失	154	144	10	37 情報セキュリティ	2366	2287	79	(f) 誠実性		
3. 与信				38 情報の可用性	1062	993	69	47 経営者の不正	1	1
26 債務不履行	1202	1190	12	39 情報技術のインフラストラクチャ	337	307	30	48 従業員の不正	2952	2891
27 取引先集中	233	214	19					49 第三者の不正	1176	1093
28 決済未了	3	3	0					50 過失	1678	1624
29 担保価値損失	506	491	15					51 無権限者による経営資源の使用	5	5
(g) 業務/運営										
52 顧客満足	199	196	3	62 流通チャネルの機能不全	1268	1240	28			
53 人的資源・資質	2146	2065	81	63 提携先の内部統制	1051	1004	47			
54 知的資産の維持活用	1313	1247	66	64 広義のコンプライアンス	1646	1554	92			
55 製品開発力	1010	978	32	65 特定の経営資源への依存	409	390	19			
56 業務効率	1021	977	44	66 製品・サービスの欠陥	2610	2549	61			
57 生産能力	2056	2033	23	67 環境への負荷・対応	1102	1067	35			
58 取引拡大への対応能力	25	23	2	68 労務問題	1323	1237	86			
59 期待パフォーマンスとのギャップ	756	724	32	69 人権問題	30	23	7			
60 サイクルタイムにおける業務効率	380	357	23	70 健康・安全管理	2161	2084	77			
61 サプライチェーン	2959	2921	38	71 商品ブランド	646	617	29			

C 意思決定情報リスク			
	FY18	FY17	差
(a) 戦略			
72 外部環境モニタリング	107	100	7
73 ビジネスモデルの陳腐化	245	235	10
74 ビジネスポートフォリオ	181	173	8
75 投資判断情報	1582	1523	59
76 組織構造の戦略整合性	2	3	-1
77 KPIの戦略整合性	6	2	4
78 経営資源の最適配分	1996	1914	82
79 戦略の外部環境適合性	565	541	24
80 製品ライフサイクルを考慮した戦略	107	108	-1
(b) 外部報告			
81 外部報告の虚偽記載	0	0	0
82 会計基準・準拠積もり	828	813	15
83 減損	843	796	47
84 財務報告の内部統制有効性評価	314	275	39
85 開示統制の整備運用	16	17	-1
86 税務戦略情報	1098	1063	35
87 年金基金情報	7	10	-3
(c) 業務/運営			
88 予算・計画統制	512	476	36
89 価格設定	3007	2959	48
90 契約履行情報	1741	1691	50
91 業績評価指標の有効性	9	6	3
92 財務業績偏重による経営管理	0	0	0

TOP10リスク

(両年度とも同じ)

1. 関連法規(外)
2. 災害(外)
3. 価格設定(戦)
4. 金融市場(外)
5. サプライチェーン(業)
6. 外部環境感応度(外)
7. 従業員不正(業)
8. 競合他社(外)
9. 製品サービス欠陥(業)
10. 情報セキュリティ(業)

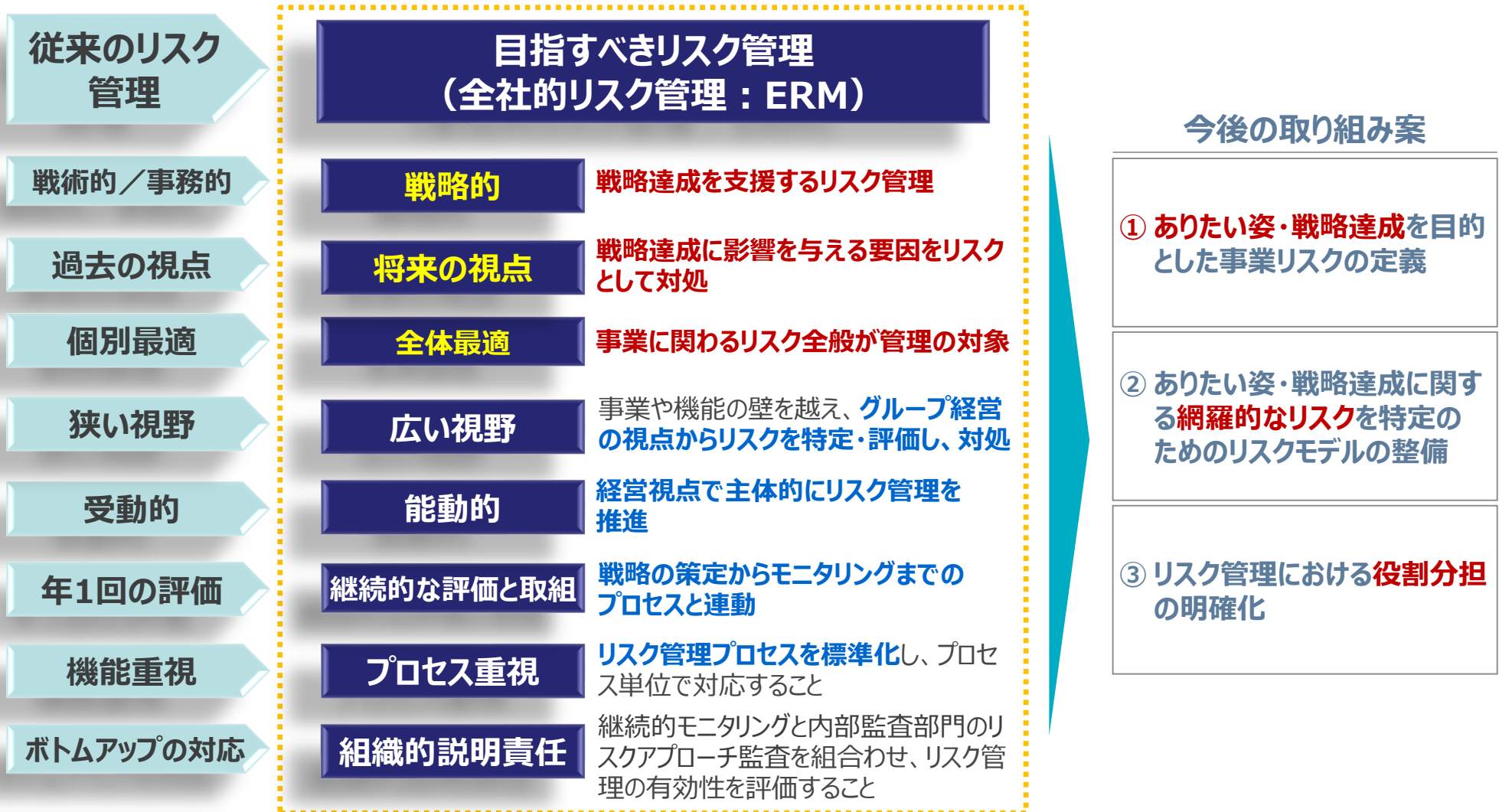
報われるリスク

報われないリスク

- 知らないことを知るーすごいこと (ソクラテス)
- 知らないことを知らないー最も怖いこと

リスク管理の全社対応に向けた今後の取り組み案

年次・中長期計画策定に戦略達成のためのリスク情報を盛り込むための体制が重要です。



リスクの定義 ～COSO*におけるリスクの定義の変遷

(○印は該当すると考えられるもの)

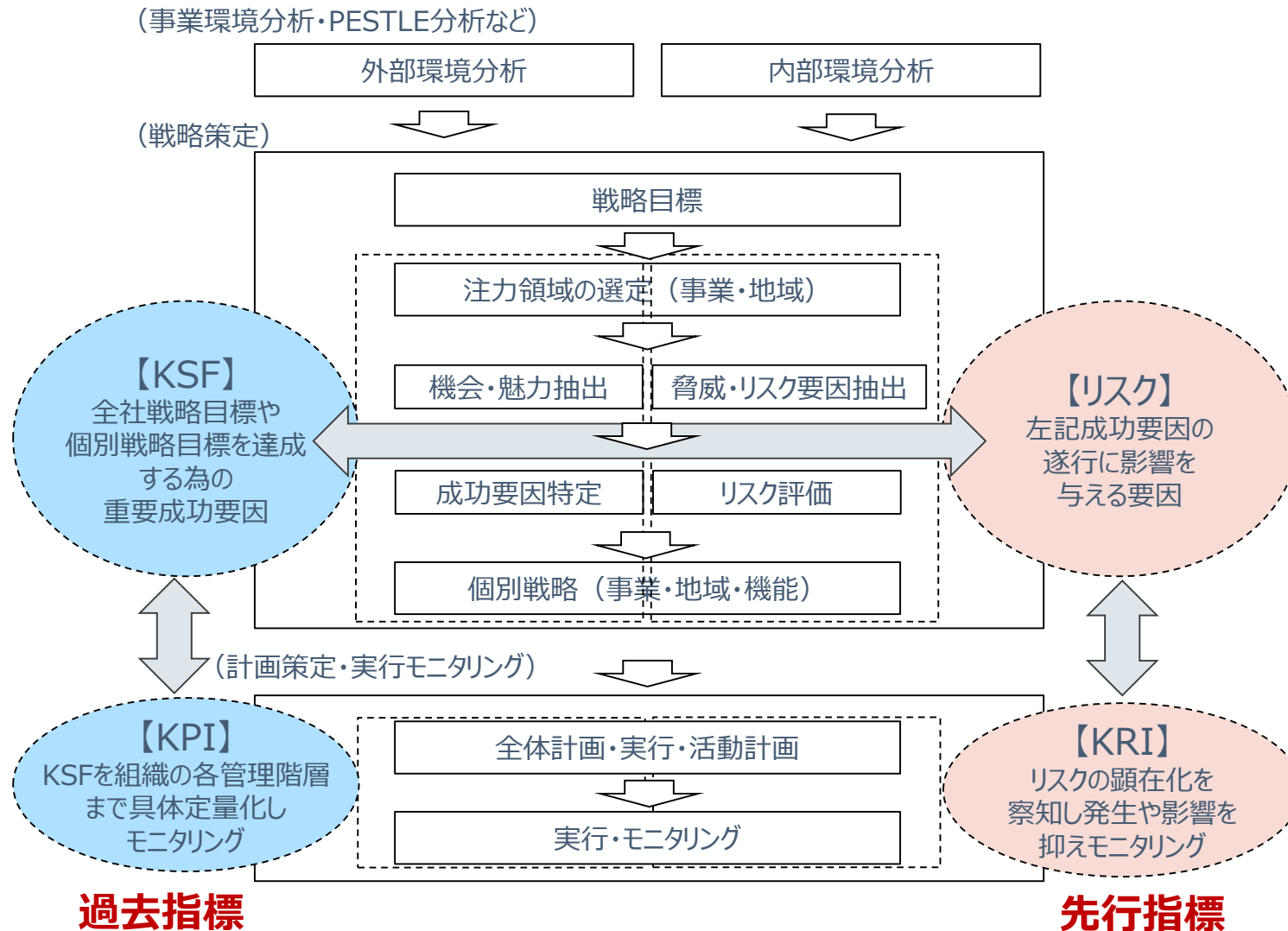
フレームワーク リスク	COSO内部統制 1992	COSO・ERM 2004	COSO内部統制 2013	COSO・ERM 2017
定義	内部統制の目的達成を 阻害 する 事象	ある事象が目的達成とは 反対 の影響を与える 可能性	事象が発生し目的の達成に 不利 な影響を及ぼす 可能性	事象が発生し戦略と事業目標の達成に影響を及ぼす 可能性
報われないリスク	○	○	○	○
報われるリスク —失敗要因	—	○	○	○
報われるリスク —成功要因	—	— (機会として定義)	—	○

*COSO : Committee of Sponsoring Organization of Treadway Commission

2. 戦略達成のためのリスクマネジメント

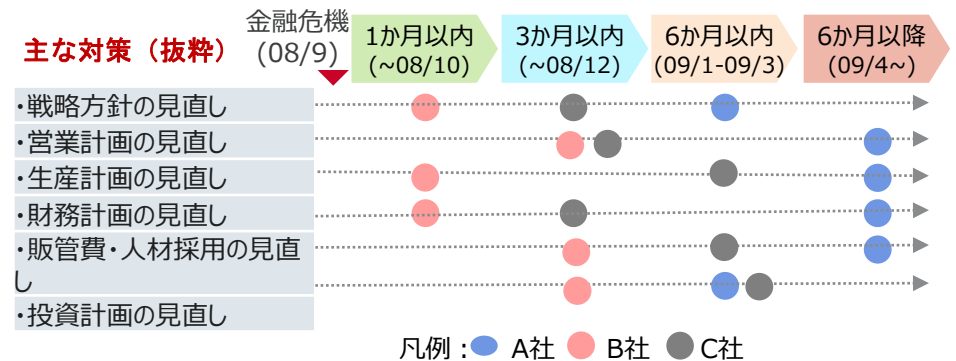
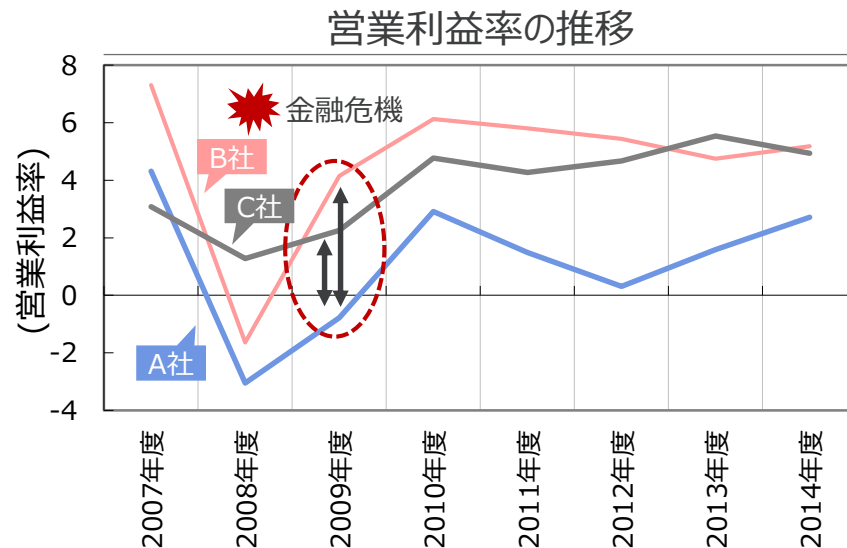
戦略策定から実行・モニタリングフローを軸とするリスクとの関連性

【戦略策定・実行・モニタリングフロー】



ERMを推進している先行企業との比較例（日本企業の例）

金融危機時、同じ業界における3社の業績回復とその後の競争上の優位性、ポジショニングをどのように確保しているか、ERMの基盤をもとに比較検証した結果、3社のリスクによるインパクトと回復動向、その後の優位性に大きな差があることが判明した。



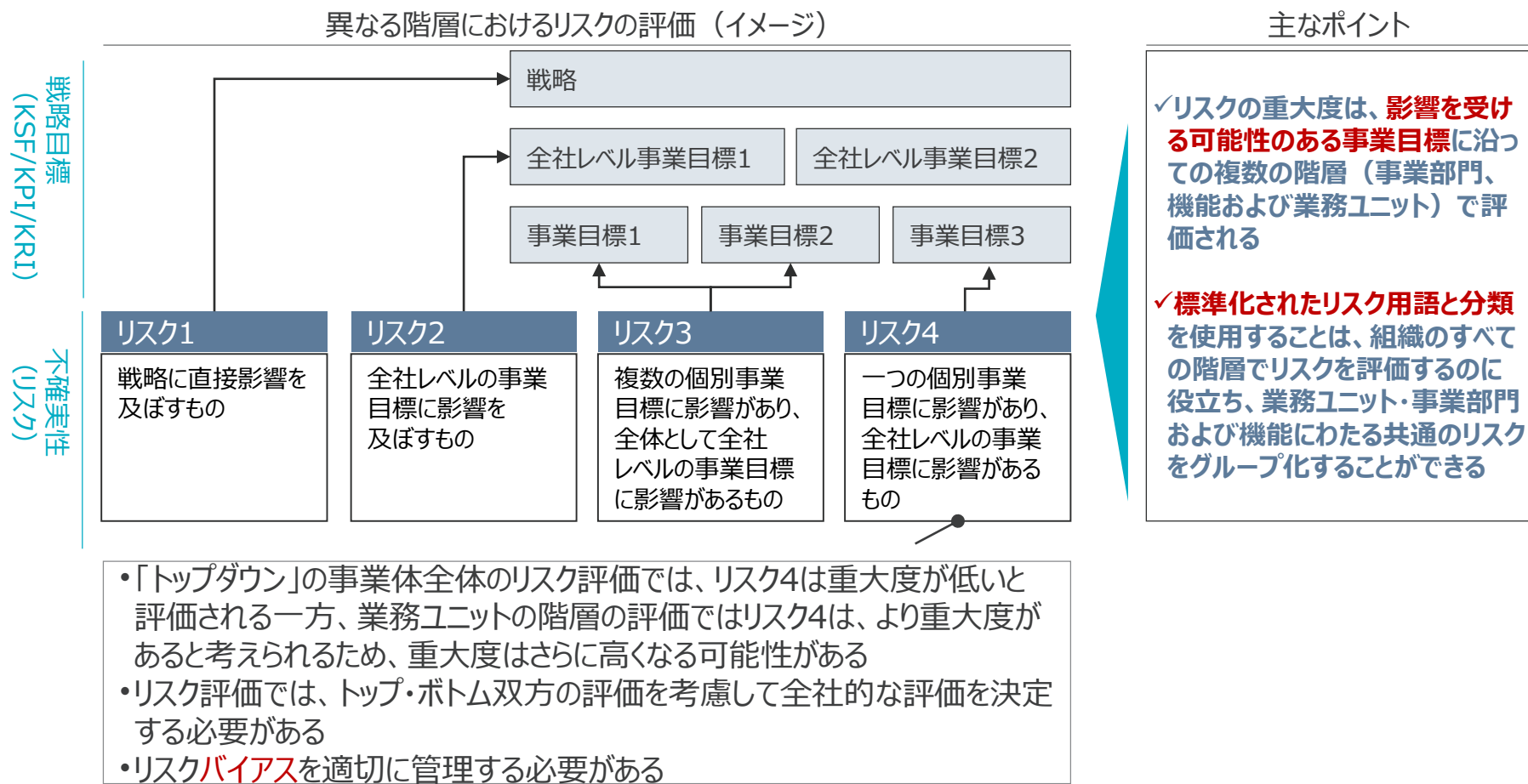
- ・ A社は、環境変化に対応する仕組みが弱かった
- ・ B社、C社はERM導入を数年に亘って整備していた
- ・ B社は特にキャッシュフローの改善に重点をおいた

ポイント

- ・ 伝統的なリスク管理をベースにしていたA社、ERMの導入を率先して進めていたB社、導入途上であったC社の、その後のポジショニングに大きな影響が出ている。
- ・ 戦略とERMの統合度合いによって、**レジリエンスの違い**が浮き彫りになったと言える。

ご参考：戦略目標とその達成におけるリスク

組織の各階層によって認識しているリスク、およびその重要度は異なるため、全社的なリスクを特定・評価する際は、階層ごとの認識を、偏りなく把握し、整理する必要がある。



ご参考：プロティビティビジネスリスクモデル

事業に関連する内外の様々なリスクを全社的に、網羅的に特定するためのツール。

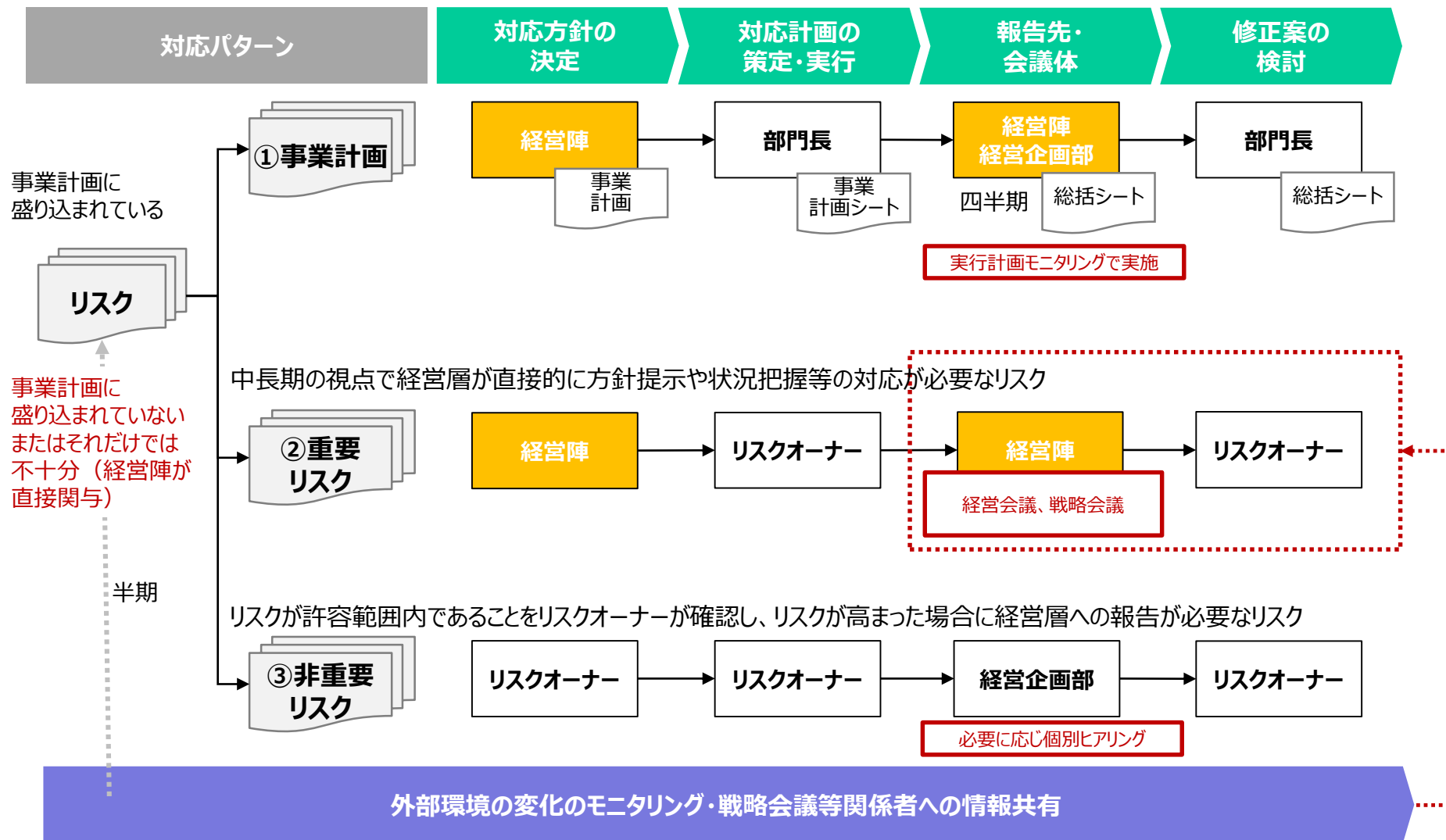
- リスクの特定をする際、**網羅的なリスクの棚卸表**として機能する。
- 特定するリスクのレベル感、**源泉を意識したリスク**の特定に役立つ。
- リスク定義を基にコミュニケーションを行うことでリスクに対する**共通認識**を形成するのに役立つ。

外部環境リスク	業務プロセスリスク			意思決定情報リスク	
<div>1.競合他社</div> <div>2.顧客の意向</div> <div>3.技術革新</div> <div>4.外部環境への感度</div> <div>5.株主の期待</div> <div>6.資本調達</div> <div>7.政体の安定性</div> <div>8.法令改変</div> <div>9.諸規則改変</div> <div>10.業界特性</div> <div>11.金融市場</div> <div>12.災害・壊滅的損失</div>	<div>財務</div> <div>価格</div> <div>13.利率</div> <div>14.外国為替</div> <div>15.投資持分</div> <div>16.商品相場</div> <div>17.金融商品</div>	<div>権限委譲</div> <div>25.リーダーシップ</div> <div>26.権限・制限</div> <div>27.アウトソーシング</div> <div>28.評価基準</div> <div>29.変化への順応性</div> <div>30.コミュニケーション</div>	<div>ガバナンス</div> <div>35.企業文化</div> <div>36.倫理的行動</div> <div>37.取締役会の有効性</div> <div>38.事業承継計画</div>	<div>戦略</div> <div>64.外部環境のモニター</div> <div>65.ビジネス・モデル</div> <div>66.ビジネス・ポートフォリオ</div> <div>67.事業価値の評価/投資判断</div> <div>68.組織構造の有効性</div> <div>69.戦略に基づく実績測定</div> <div>70.経営資源配分</div> <div>71.戦略策定</div> <div>72.製品ライフサイクル</div>	
	<div>流動性</div> <div>18.キャッシュフロー</div> <div>19.機会損失</div> <div>20.市場の集中</div>	<div>情報処理/IT</div> <div>31.完全性</div> <div>32.アクセス</div> <div>33.可用性</div> <div>34.インフラストラクチャ</div>	<div>評判</div> <div>39.イメージ/ブランド力</div> <div>40.利害関係者</div>		<div>誠実性</div> <div>41.経営者の不正</div> <div>42.従業員の不正</div> <div>43.第三者の不正</div> <div>44.違法行為</div> <div>45.無権限者による使用</div>
	<div>与信</div> <div>21.債務不履行</div> <div>22.取引先の集中度</div> <div>23.決済</div> <div>24.担保価値</div>	<div>業務/運営</div> <div>46.顧客満足</div> <div>47.人的資源</div> <div>48.知的資産</div> <div>49.製品開発</div> <div>50.業務効率</div> <div>51.処理(生産)能力</div> <div>52.量的拡大への対応</div> <div>53.パフォーマンスギャップ</div> <div>54.サイクルタイム</div>			<div>55.外部からの調達</div> <div>56.流通チャネルの有効性</div> <div>57.提携先</div> <div>58.コンプライアンス</div> <div>59.ビジネスの中断</div> <div>60.製品・サービスの欠陥</div> <div>61.環境問題</div> <div>62.健康・安全管理</div> <div>63.商標・ブランド劣化</div>
					<div>外部報告</div> <div>73.財務報告の評価</div> <div>74.内部統制評価</div> <div>75.経営者の宣誓</div> <div>76.税務情報</div> <div>77.年金基金</div> <div>78.監督機関への報告</div>
					<div>業務/運営</div> <div>79.予算・計画</div> <div>80.価格設定</div> <div>81.契約条項</div> <div>82.業務測定</div> <div>83.目的・戦略との整合性</div> <div>84.会計情報の偏重</div>

ビジネス リスクモデルの特長

- ✓ 特定の業種に依らない汎用的モデル
- ✓ 網羅的に84のビジネスリスクの例示
- ✓ リスク毎にリスクのシナリオを定義。
- ✓ 結果ではなく源泉を基に整理され、その後の活動につなげやすい

ご参考：リスク評価結果の事業計画等への組み込み（例）



取締役会はどこで関与し、ガバナンス機能を発揮すべきか？

ERMの推進体制

各社によってERMの構築・高度化に適した体制は異なるため、自社におけるERMを構築・高度化のプロジェクトを成功に導きやすい体制を検討する必要があります。

現状のリスク管理の推進体制

専門部門が担当
(リスク管理部、
ERM部等)

企画部門が兼務
(経営企画部等)

非企画部門が兼務
(法務部、総務部等)



ERMの構築・高度化の プロジェクト体制

既存の主管部門が推進

複数部門で
プロジェクトチームを
結成して推進

プロジェクト体制に求められる要件

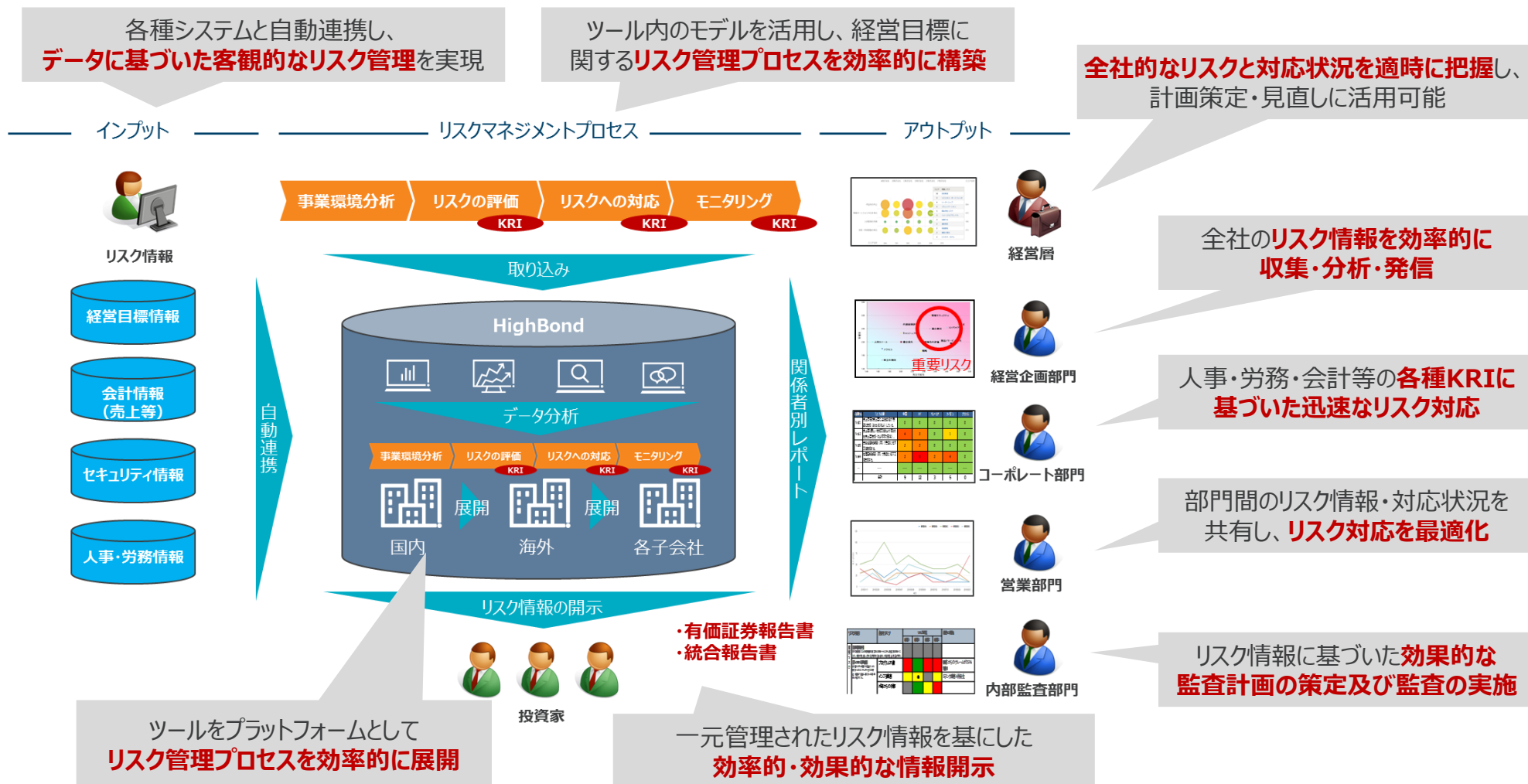
- ✓ ERM推進に関して、経営陣の理解と強いコミットを得られる
- ✓ 事業部門を含めた全社的な連携（巻き込み）をスムーズに実施できる
- ✓ プロジェクト推進にフルコミット出来る一定の人員や、適宜外部専門家を活用出来る予算を確保できる
- ✓ 構築・高度化の取り組み後も継続的にフォローアップ（仕組みの定期的な見直し・改善）できる（プロジェクトチームで推進する場合は、運用が安定次第担当部門を設定し・委任することを想定）

ご参考：ERM推進アプローチ

フェーズ	1. ミッション・ビジョン・戦略の明確化	2. 戦略達成に係る全社的リスク評価	3. リスク対応計画の策定	4. リスク対応の実施・モニタリング
タスク概要	<p>ERMの目的設定</p> <ul style="list-style-type: none"> ERMに対する期待やERM推進の目的を明確化 <p>リスク管理体制の整備</p> <ul style="list-style-type: none"> リスク管理所管部署や報告経路等を整備 <p>ミッション・ビジョンの確認</p> <ul style="list-style-type: none"> 組織のミッション・ビジョン・行動指針等、長期的な方向性を確認 <p>戦略及び事業目標の整理</p> <ul style="list-style-type: none"> ミッション・ビジョンを実現するための経営戦略・事業目標について、それぞれの関連性や階層関係を把握し、必要に応じて見直し 	<p>リスク評価の共通言語の設計</p> <ul style="list-style-type: none"> リスクを網羅的に洗い出すためのモデル、リスクの重要性を評価するための評価基準等を設計 <p>事業環境分析</p> <ul style="list-style-type: none"> リスク評価者の共通理解を図るため、組織内外の事業環境分析を実施 <p>リスクの特定・評価</p> <ul style="list-style-type: none"> 戦略達成に係るリスクを特定し、対応すべきリスクを優先順位づけ 	<p>リスクオーナーの設定</p> <ul style="list-style-type: none"> リスク対応計画を策定するリスクオーナーを設定 <p>リスク対応状況の把握</p> <ul style="list-style-type: none"> リスクへの対応を検討するため、現状のリスク対応状況を把握 <p>リスク対応計画の策定</p> <ul style="list-style-type: none"> リスク対応状況を踏まえ、リスクへの対応計画を策定 	<p>モニタリング体制の構築</p> <ul style="list-style-type: none"> リスク対応計画の進捗状況をモニタリングするための体制・モニタリング項目・頻度等を設計 <p>対応の実施・モニタリング</p> <ul style="list-style-type: none"> リスクオーナーが対応計画を実施し、対応状況についてモニタリング <p>RMの有効性評価</p> <ul style="list-style-type: none"> RMの有効性を全社的な視点から評価し、更なる高度化を検討 <p>RMの情報開示</p> <ul style="list-style-type: none"> RMの実施状況について、有価証券報告書や統合報告書等での開示内容を検討
資料データ例	<ul style="list-style-type: none"> ERM研修資料 戦略体系 リスク管理体制図 	<ul style="list-style-type: none"> リスクモデル リスク定義 リスク評価基準 事業環境分析資料 リスクシナリオ一覧 リスク評価結果 	<ul style="list-style-type: none"> リスク管理の役割分担表 リスクオーナー一覧 リスク対応計画 	<ul style="list-style-type: none"> モニタリングフォーマット モニタリング体制図 RMの有効性評価項目 RMの有効性評価結果

ご参考：“Digital ERM” のビジョン

Digital ERMは、グループ全体のリスクマネジメントプロセスを高度化・効率化し、経営層のみならず各部門の意思決定に有用な情報を提供することで、リスク対応の早期化・最適化を実現します。

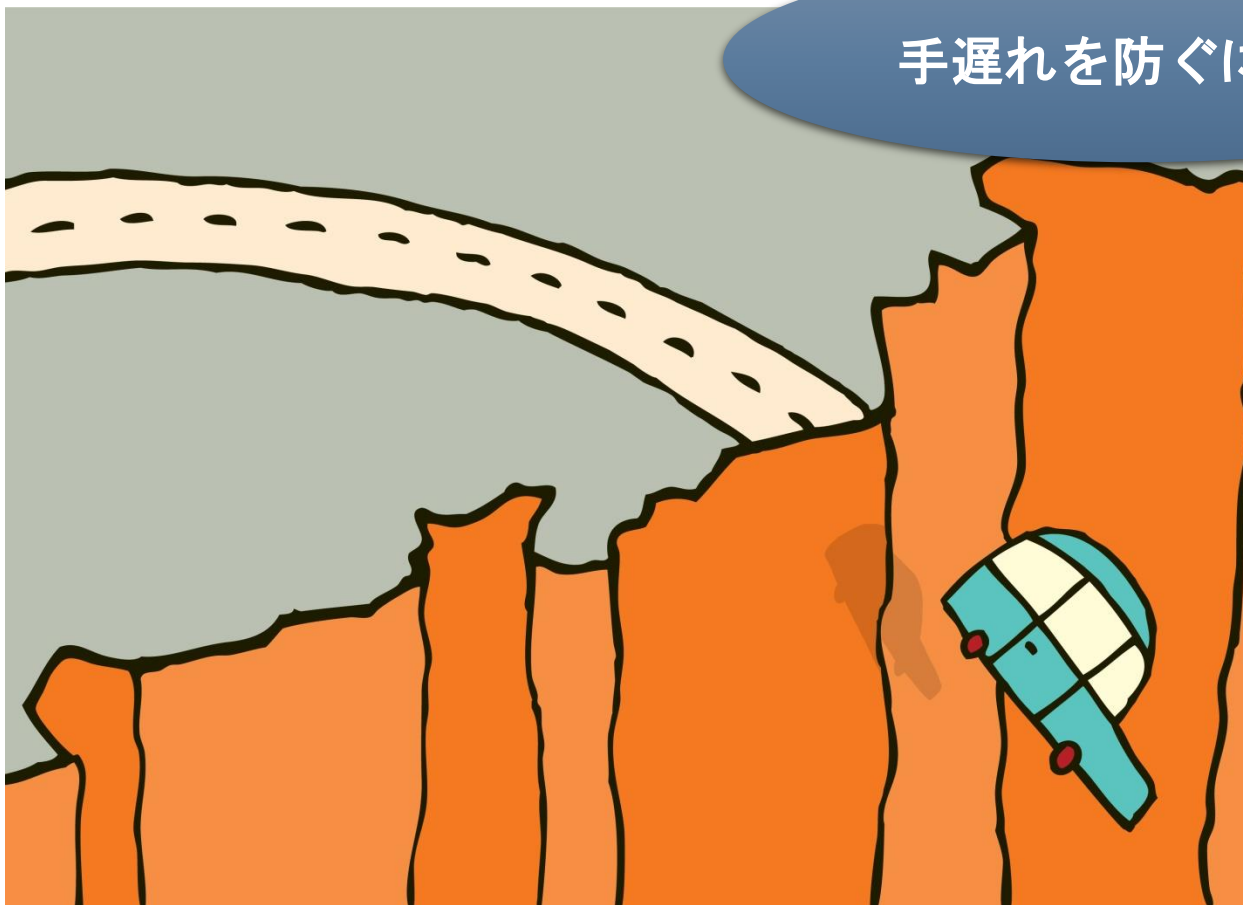


仮説指向プランニング

意思決定までは、大騒ぎで議論をするが、その後は、
事業チームに任せきりで、取締役会に進捗報告もなく、
いつの間にか失敗している

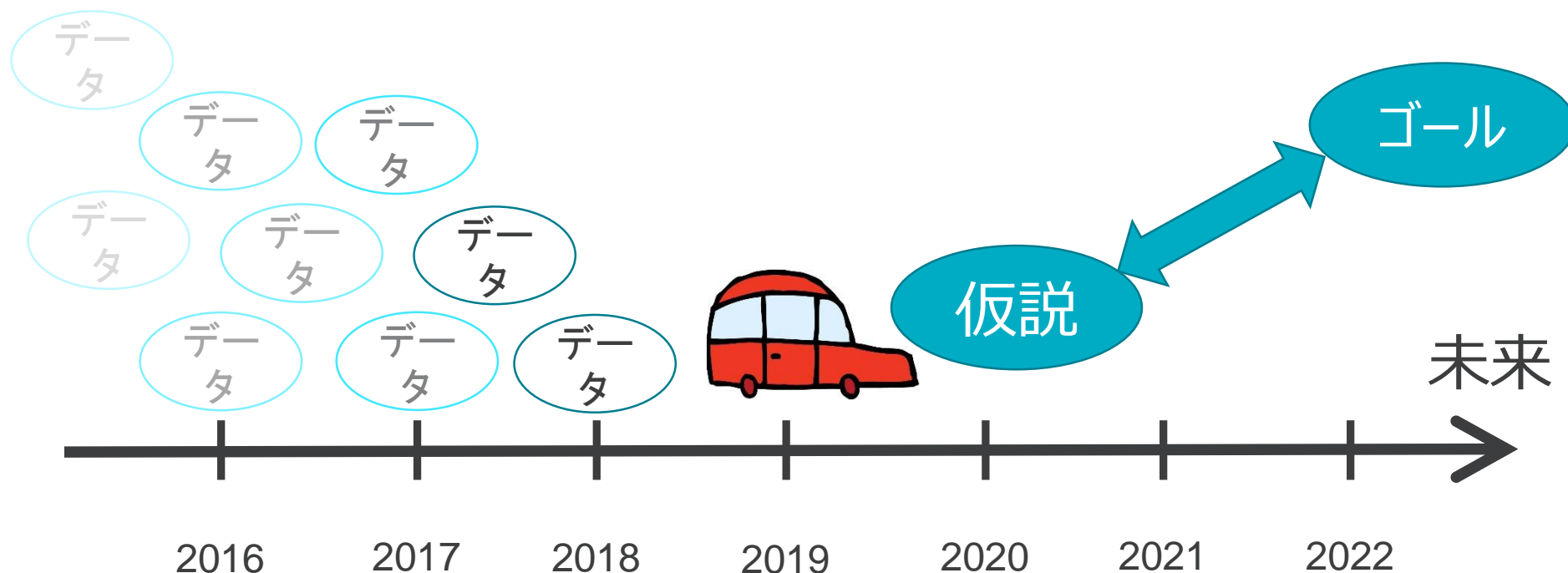
手遅れを防ぐには？

HARD THINGS
ベン・ホロウィッツ
日経BP社
の記述より



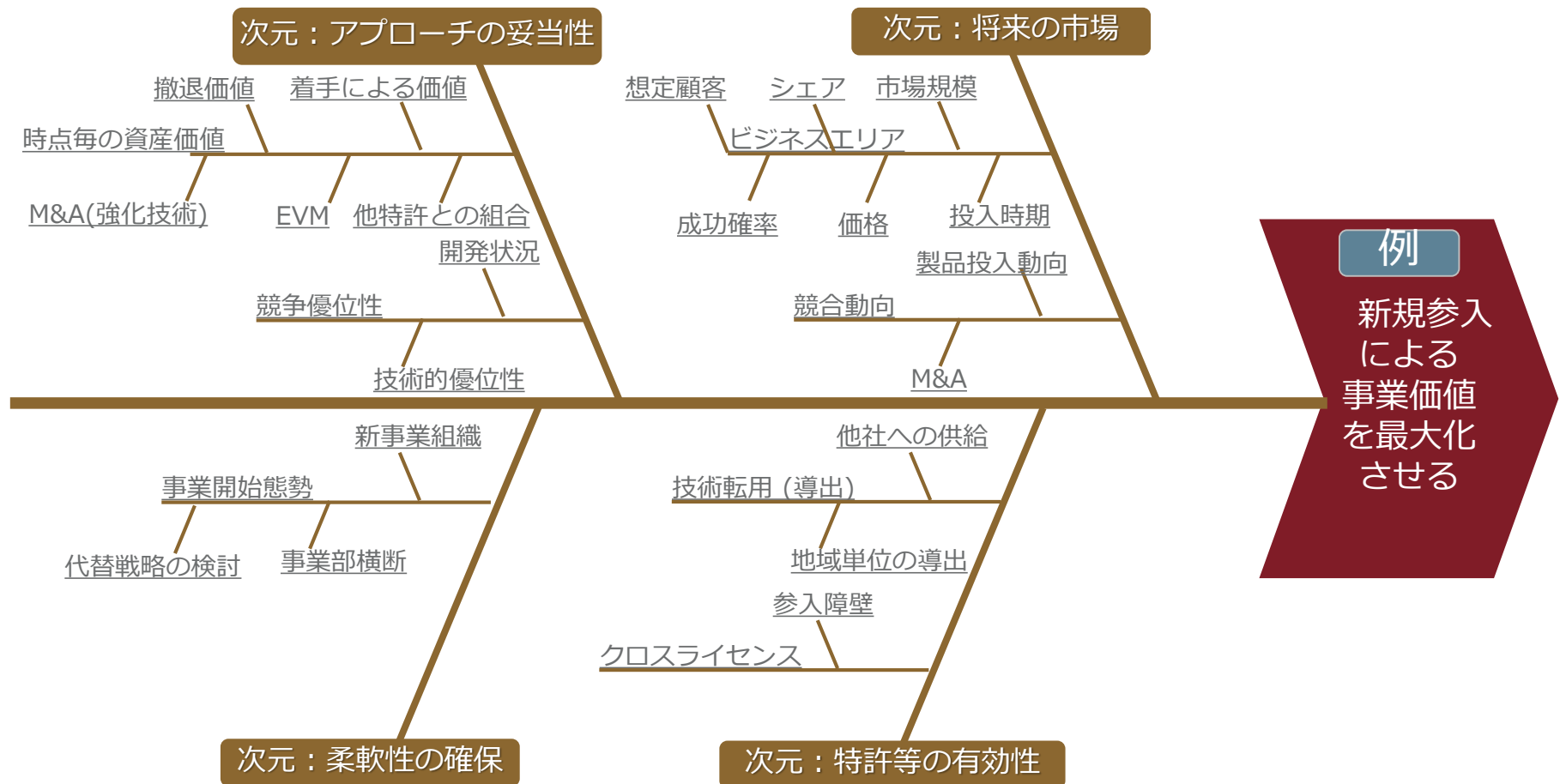
ゴールを目指し、仮説を指向する経営を推奨します

仮説が「現在」と「ゴール」を
結び付ける



戦略実現をより確実にすべく ～リスクシナリオとKPI・KRIのモニタリング

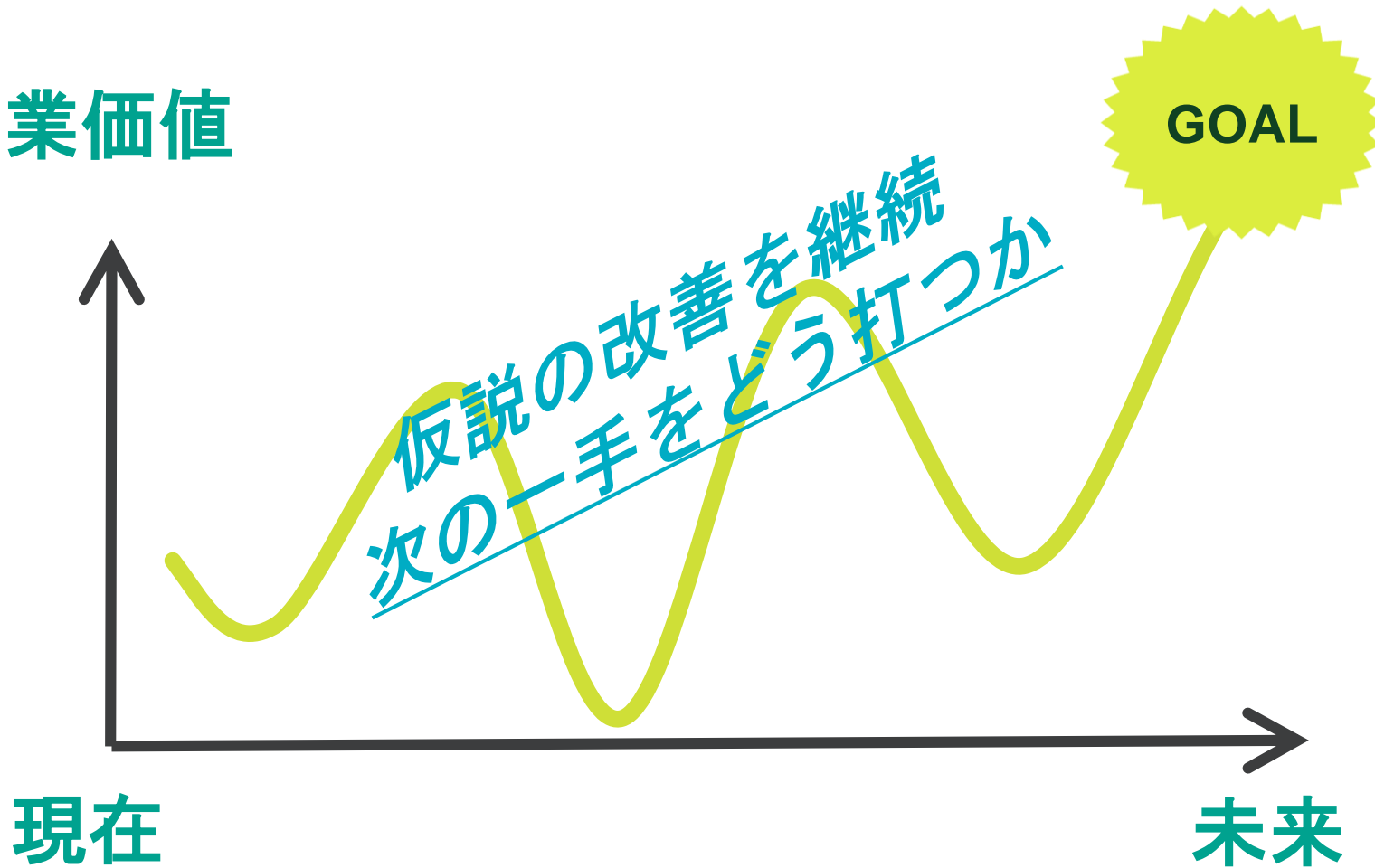
戦略の前提条件・仮説を分析整理し、効果的なモニタリングを行うには、「Fish Bone」等のツールを用いて可視化し、次元ごとの必要なデータを特定と適切な**KPI・KRI**の設定



ご参考：その仮説は、まだ生きていますか？

次の選択肢の検討と意思決定の繰り返し

事業価値



ご参考：DDP*～計算に用いた数値の設定根拠を継続的に管理する

ここが大切！

仮説名	設定根拠（仮説）	Base	Low	High
2022年までの販管費低減率目標	過去の実績を勘案し…	0%	-4%	0%
2022年までの原価低減率目標	x x部ヒヤリングより…	0%	-3%	0%
企業内設置市場規模 2022	調査会社Aの資料に…	60,000	20,000	100,000
製品価格 2022	他案件と妥当性を…	¥300 k	¥200 k	¥360 k
企業内設置 マーケットシェア 2022	半年毎の検証を継続…	17%	13%	34%
2023年以降の売上高成長率	High達成の前提は…	0%	0%	15%
一般家庭市場規模 2022	調査会社Aの資料に…	10,000	1,000	20,000
公共機関 マーケットシェア 2022	シェア拡大具体策は…	14%	10%	30%
公共機関市場規模 2022	調査会社Aの資料に…	30,000	14,000	50,000
その他市場規模 2022	調査会社Aの資料に…	10,000	4,000	20,000
ライン当たり光熱費 2022	Low達成には…	2	1.6	2.4
注文当り必要訪問回数 2022	事前検証が不可欠…	7	5	10
一人当り訪問可能回数 2022	調査によって、精度…	2	1	3
初期投資 2018		20	契約によって確定済	

*DDP：Discovery Driven Planning

ご参考：AIなど最新データにより、仮説の外れに対応する仕組みを構築 組織の役割分担に基づく仮説検証型マネジメント



この過程で財務規律などガバナンス機能はどのように発揮すべきか

3. ESG/SDGs リスクへの対応

ESGリスクへの対応 ～COSO・ERM2017を活用

ESGに関する取り組み促進は企業の**中長期戦略**にも深く関わり、COSO・ERM2017は、戦略との統合を念頭に入れ、ESG関連リスク管理のガイダンス*を提供しています。



ESGリスクは、**定量化が難しく**、知識不足などが原因で、他のリスクより特定が難しい傾向にある

マクロ的で複雑なため、より予測が難しく、**長期的**なリスクである

過去に顕在化していないため、**過去データによる評価は難しい**

低減や排除は難しく、リスクの顕在化への対応として**レジリエンス**を高める必要がある（BCPやシナリオ法の更なる活用）

***ERM ESGガイダンス（2018年10月）は、COSOとWBCSDが共同で作成し、WBCSD**は、会員企業に当ガイダンスの実効的な採用を強く推奨している。**

****** 持続可能な開発のための世界経済人会議: World Business Council for Sustainable Development

ESG/SDGs対応 成熟度モデル

ESG成熟度

Protiviti 独自の環境経営 ESG・Sustainability 成熟度モデル

変革者

リーダー

追従者

出遅れ

フォーカス

リップサービス

規制対応

効率性

戦略的

統合

四半期単位

長期的視点

「いつもどおり」のまま

- ・位置付け：
 - 地域社会との関係
 - 慈善活動
- ・適切な発言
- ・場当たりの対応
- ・「その場しのぎ」の解決策
- ・危機が生じた際に対応

規制遵守

- ・位置付け：
 - 純粋なコンプライアンス
 - 事業活動の周辺
 - 縦割り
- ・方針とプロセスを策定
- ・コスト要因との捉え方
- ・目立たない存在

予防への注力と無駄の排除

- ・位置付け：
 - 企業全体にわたる品質イニシアティブ
 - 財務的パフォーマンスの改善要因
 - 基準設定と実施
- ・コスト削減を目標に
- ・望ましい行動を定め、促進
- ・達成が容易な目標を追求
- ・サステナビリティ報告は負担との捉え方

ESGレピュテーションとブランドイメージの構築

- ・位置付け：
 - 競争優位の源泉
 - 企業にとって不可欠
 - 経営陣の責任
 - ESG投資としての選択肢
- ・以下の事項を重視
 - 明確なESGビジョンを確立
 - ビジョンを目標設定に組入
 - ESG目標を戦略設定に組入
 - 結果に対する説明責任を確立
 - 中核的能力を構築
- ・効果的なアウトリーチを実施
 - 従業員
 - 顧客
 - バリューチェーン（サプライヤー、物流、チャネル）
 - 公的セクター
 - 地域社会
- ・サステナビリティ報告は機会との捉え方

ビジネスモデルの変革

- ・位置付け：
 - 長期的な企業存続を可能にする要因
 - 企業のDNAと文化の中核
 - CEOの責任
 - ESG関連投資の最高かつ最善の適用
- ・企業家的行動を体系的思考を通じて促進し、イノベーションに焦点を当てる：
 - プロセス
 - 製品
 - サービス
- ・将来世代の健康と活力を維持するための共同イニシアティブを支援
 - 複数のステークホルダー
 - 公的セクター
 - 業界
 - グローバル
- ・サステナビリティ報告は、ストーリーを伝えるために不可欠との捉え方

ご参考： 分析手法例

～COSO・WBCSD 「COSO・ERMのESG リスクへの適用」 の活用

章	行動
1	ESG関連リスクに関するガバナンスとカルチャー
	<input type="checkbox"/> 組織の必須または任意のESG関連要件をマッピングまたは定義する。 <input type="checkbox"/> ESGを事業体のカルチャーやコアバリューに組み込む機会を検討する。 <input type="checkbox"/> ESG関連リスクに対する取締役会の認識を高める方法を知らせる。 <input type="checkbox"/> 事業構造、ESG関連リスクのリスクオーナー、報告経路、ERMの全貌、および戦略策定プロセスをマッピングして、監視と連携を改善するための領域を識別する。 <input type="checkbox"/> 組織全体で連携の機会を創出する。 <input type="checkbox"/> 統合を促進するためにESG関連のスキル、能力および知識を、採用およびタレントマネジメントに組み込む。
2	ESG関連リスクに関する戦略と目標設定
	<input type="checkbox"/> 価値創造プロセスとビジネスモデルを検討し、短期、中期、長期にわたるすべての資本への影響と依存関係を理解する。この理解を助けるために以下を行う。 <ul style="list-style-type: none"> - 外部環境における新たな問題の影響を理解するためのメガトレンド分析 - 強み、弱み、機会、および脅威（SWOT）分析 - あらゆる種類の資本に対する影響と依存関係のマッピング - ESGの重要な問題を説明するためのESGの重要性評価 - 新たなESGの動向を理解するための内外のステークホルダーとの関係構築 - ESG固有の資源を活用した分析 <input type="checkbox"/> リスクマネジメントプロセス全体を通して、事業体の戦略、目標、およびリスク選好を整合させる。 <input type="checkbox"/> 事業体の戦略や目標に影響を与えるESG関連リスクを検討する。
3	ESG関連リスクに関するパフォーマンス
3a	リスクを識別する
	<input type="checkbox"/> 事業体のリスク一覧表を調べて、どのESG関連リスクが識別されたか、または識別されなかったかを確認する。 <input type="checkbox"/> ESGリスクのオーナーとサステナビリティの担当者をリスク識別プロセスに関与させて、主題に関する専門知識を活用する。 <input type="checkbox"/> ESG関連リスクを理解するために、リスクマネジメントおよびサステナビリティの双方の担当者が集う会合を開催する。 <input type="checkbox"/> 組織の戦略計画および事業計画に影響を与えるかもしれないESG関連リスクを識別する。 <input type="checkbox"/> 組織へのESG関連リスクの影響を明確にする。 <input type="checkbox"/> 根本原因分析を用いてリスクの要因を理解する。
3b	リスクを評価し、優先順位づける
	<input type="checkbox"/> リスク評価で要求される成果（例えば、戦略と事業目標の観点からの影響）を理解する。 <input type="checkbox"/> リスクの優先順位づけについての事業体の規準を理解する。 <input type="checkbox"/> リスクを表現するために事業体を使用する測定基準（すなわち、定量的または定性的）を理解する。 <input type="checkbox"/> リスクの重大度を測定するための適切な評価方法を選択する。 <input type="checkbox"/> データ、パラメータおよび前提を選択し、文書化する。 <input type="checkbox"/> ESG関連リスクに優先順位づけるために主題の専門知識を活用する。 <input type="checkbox"/> ESG問題に対する組織のバイアスを識別し、それに取り組む。
3c	リスク対応を実施する
	<input type="checkbox"/> 事業体固有の要因（例えば、費用と便益、およびリスク選好）に基づいて適切なリスク対応策を選択する。 <input type="checkbox"/> 対応のためのビジネスケース（企画書）を作成し、了承を得る。 <input type="checkbox"/> 事業体のリスクを管理するためのリスク対応を実施する。 <input type="checkbox"/> 事業体のリスクプロファイルに対する全体的な影響を理解するために、事業体レベルでリスク対応を評価する。
4	ESG関連リスクに関するレビューと修正
	<input type="checkbox"/> 戦略または事業目標に実質的に影響を与える可能性のある内部および外部の変化を識別し、評価する。 <input type="checkbox"/> ERM活動をレビューし、ERMプロセスと能力の修正すべき点を識別する。 <input type="checkbox"/> ERMによるESG関連リスクの管理方法の改善を図る。
5	ESG関連リスクに関する情報、伝達および報告
	<input type="checkbox"/> 内外のコミュニケーションおよび報告のための関連情報とコミュニケーションチャンネルを識別する。 <input type="checkbox"/> 意思決定のために、適切なESG関連のリスク情報を内部に伝達し、報告する。 <input type="checkbox"/> 規制上の義務を果たし、ステークホルダーの意思決定を支援するために、適切なESG関連のリスク情報を外部に伝達し、報告する。 <input type="checkbox"/> 内外で報告されたESG関連データの質を改善する機会を継続的に識別する。

ご参考：中長期的な社会課題の解決に関する新規ビジネス創造の例

●金属会社の例

- 中長期的な社会課題
 - 宇宙産業の規模拡大、宇宙ゴミ（スペースデブリ）の増加



- 強みを活かした新規ビジネス
 - 自社のリサイクルならびに金属回収技術を宇宙分野に適用し、宇宙ゴミの回収並びにレアメタルの回収ビジネスリーダーとなる



●産業システム関連会社の例

- 中長期的な社会課題
 - 都市部の過密化・交通量の増加による交通渋滞の増加



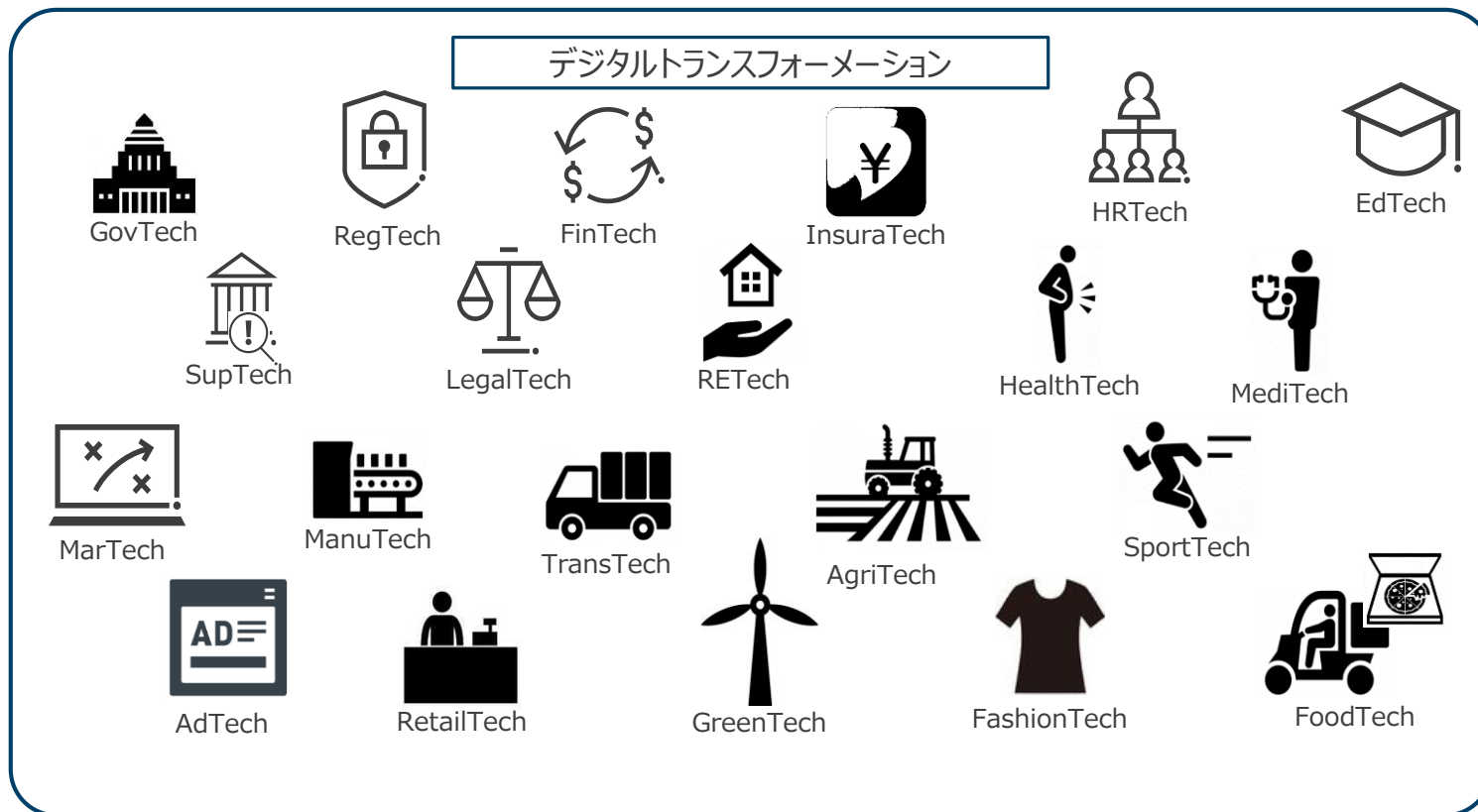
- 強みを活かした新規ビジネス
 - エレベーターパーキングの技術と国内の導入実績を活かし、海外の駐車場設置義務の規制強化による需要の拡大に応える



4. DXとサイバー・セキュリティリスク ~Digital Transformation

各分野で進むデジタルトランスフォーメーション

- デジタルトランスフォーメーション：DXとはデジタルを活用して、業務を変革すること。単なるデジタル化から次のステップへと進化している。
- DXは、既存のビジネスモデルを破壊し、組織文化を変えていく。



DXの目的

- ビジネスのDXは、主に下記の4つの目的で推進されている。
- テクノロジーの活用にとどまらず、経営陣は現状を打破し、組織がイノベーションを起こすことを求めている。



顧客エンゲージメントの改善

顧客とより深い関係を築くための、新しい方法



製品やサービスのデジタル化

製品のデジタル化および新しいビジネスモデル



より根拠のある意思決定

効果的データに基づく意思決定



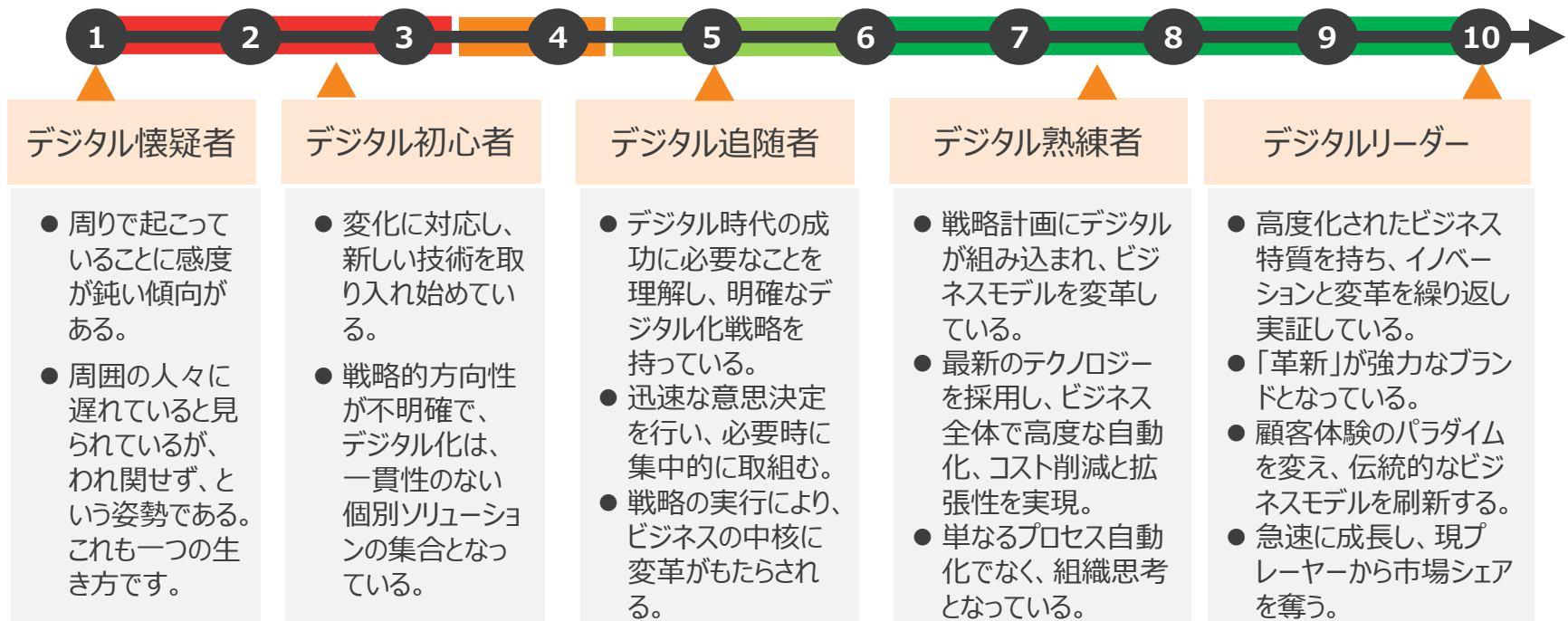
事業の効率化

テクノロジー活用によるパフォーマンスの改善

デジタル成熟度を理解する

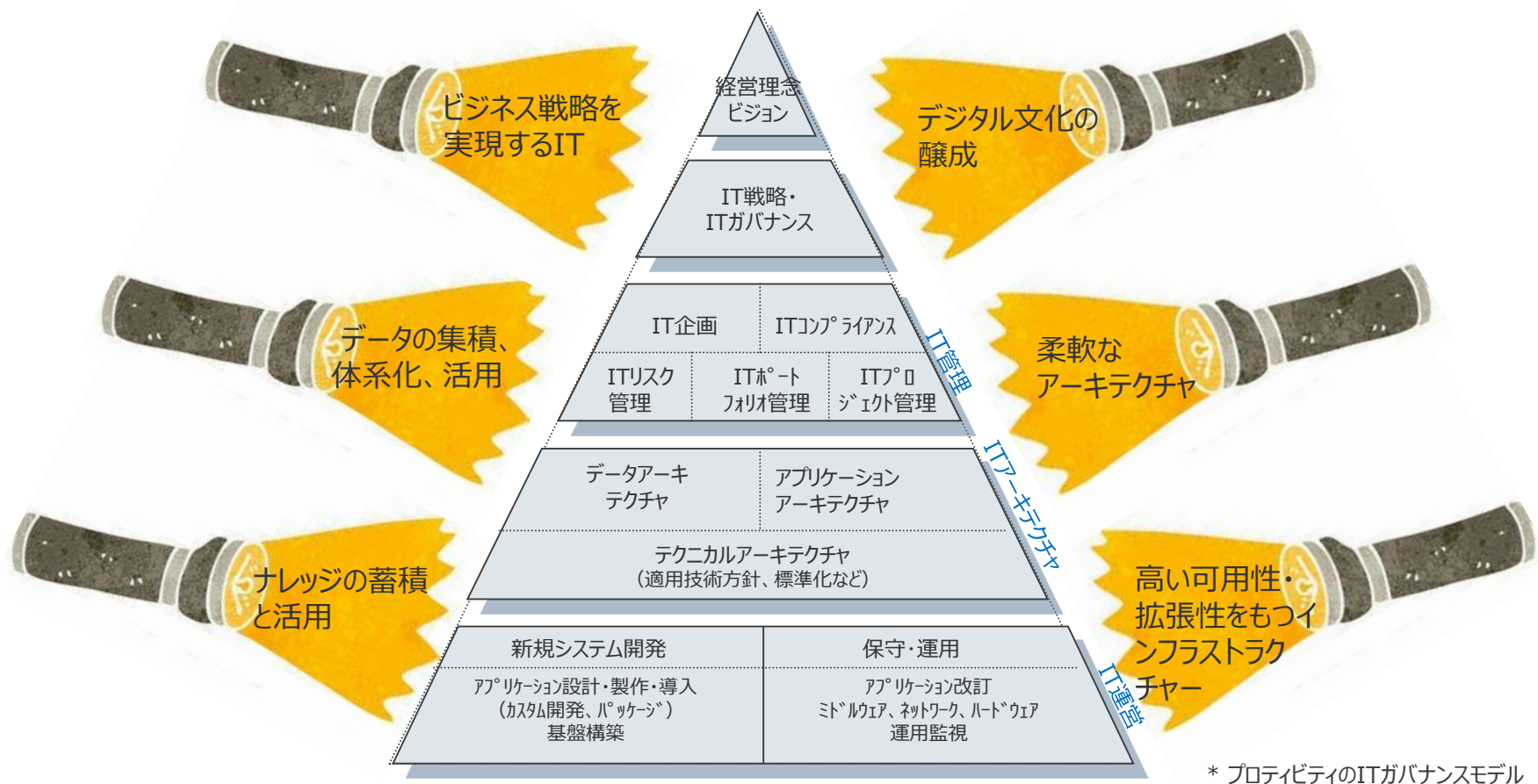
- 時間をかけてDXを経験するか、戦略的にDXを推進するか
- DXに乗り遅れると人材獲得や企業存続リスクに直結する一方、DXの最前線ではゴールは常に変化し様々なリスクにさらされる。
- 個々の企業のDXビジョンがいっそう重要に

36の能力を考慮するProtivitiのデジタル成熟度フレームワーク：



ご参考：DXを支えるIT機能の状況を把握する

IT戦略・ITガバナンスから、IT管理、IT運営まで、企業のITがどのようなリスクに直面するかを知る必要があります。



ご参考：DXのリスクを知る

企業によってDXの内容も成熟度も異なるため、自社のデジタル化によって発現するリスクが何かを独自に知る必要があります。

1 デジタル文化

2 ビジネスへの貢献

3 顧客への対応、接点
の変化

4 ITガバナンス

5 データガバナンス拡大

6 技術トレンドの追随

7 サイバーセキュリティ

8 法令遵守

9 外部委託先管理

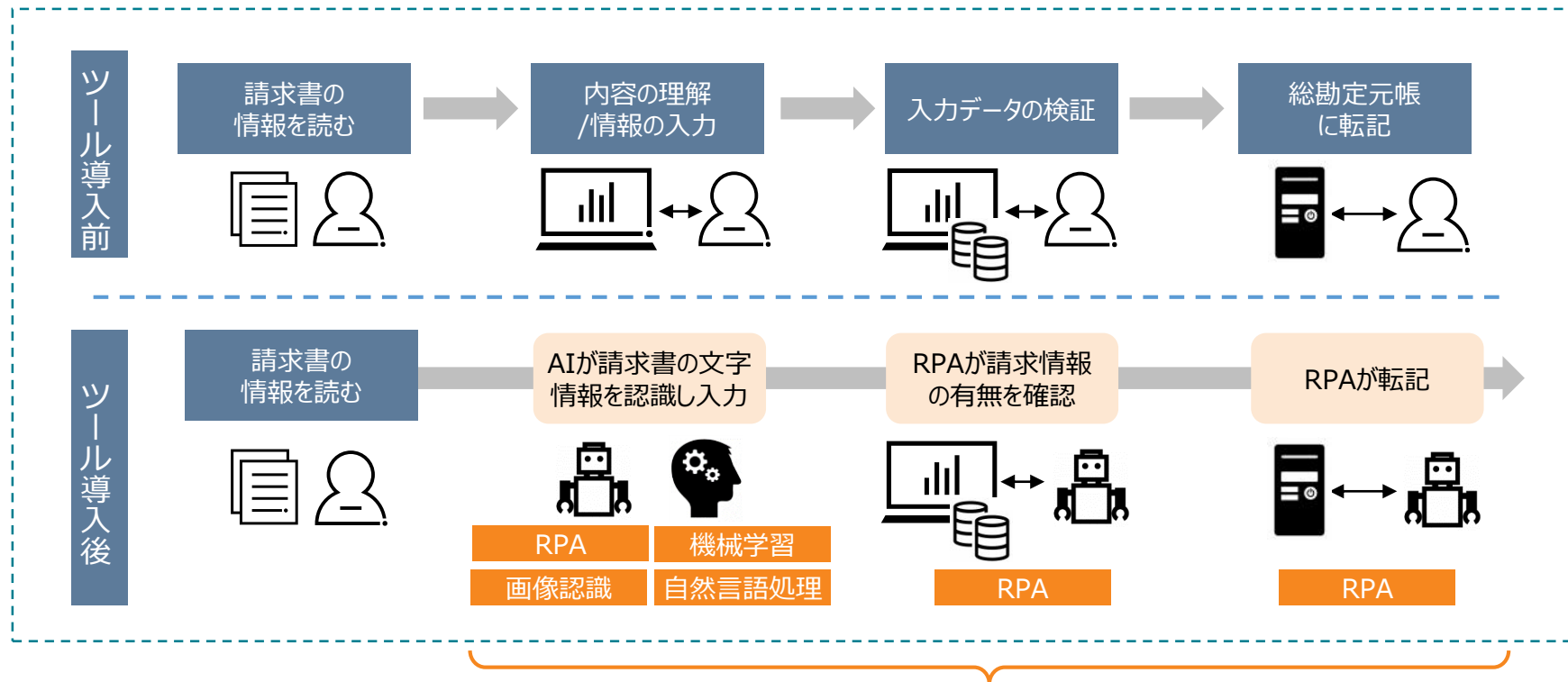
10 ITのグローバル化



11 変更、移行、
プログラムリリース

ご参考：デジタル化によるリスクの変化 ～RPAのケース

例えば、業務プロセスのDXでは、RPAによる手作業の自動化を行うと、IT業務処理統制リスクが生まれます。



IT業務処理統制リスク



不具合で機能しないリスク



勝手に変更されるリスク

規制強化の流れ：

セキュリティ・プライバシーリスクが高まる中、世界中の国や地域で規制が強化

- サイバー攻撃や個人情報保護における脅威が増え、国内外で法規制や取締りが強化
- 個人情報保護関連のコンプライアンス対応遅れは、機会喪失に加え高額な制裁金
- 海外グループを含むセキュリティ規制対応は日本主導の個別対応は非現実的
- グローバルポリシー策定とリソースの適材適所の配置が効率的モニタリングに直結

- ✓ 個人の権利範囲の拡大
- ✓ 厳格な管理と説明要件と罰則
- ✓ 規制国以外の地域にも適用



- ◆ 個別解釈による対応は危険
- ◆ スピード感
- ◆ 特定地域で個別に対応する問題ではない

ご参考：世界地図から見た個人情報保護関連のコンプライアンス

グローバルで一体化したプライバシーリスク管理が求められています。



日系企業の進出が多い地域の対象規制

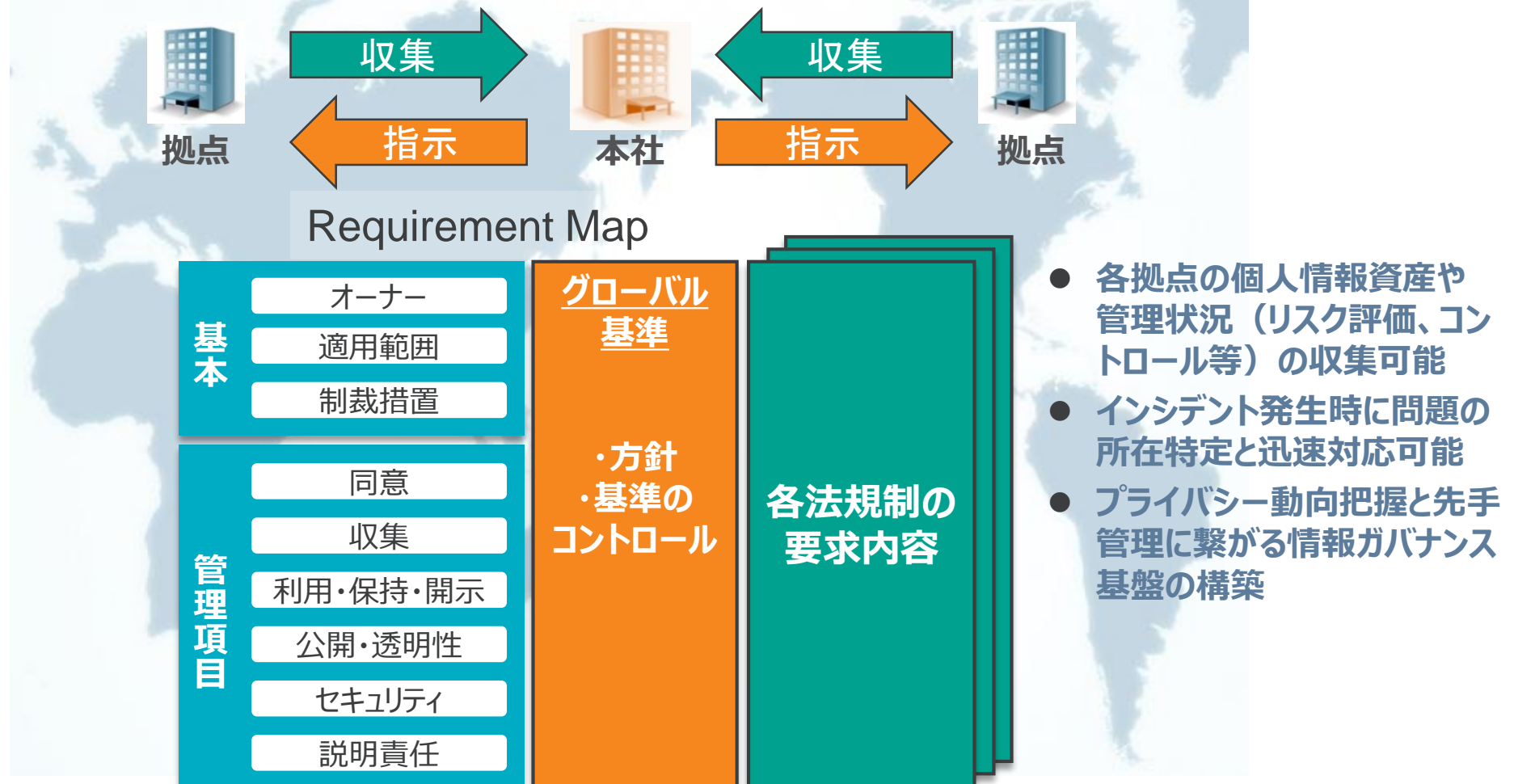
- eプライバシー規制 (EU) Cookie法
- カリフォルニア州消費者プライバシー法 (アメリカ) CCPA
- 個人情報保護および電子文書法 (カナダ) PIPEDA
- 個人情報保護法 (シンガポール) PDPA など

ご参考：法規制情報の一元管理体制の構築

戦略・
方針

プロ
セス

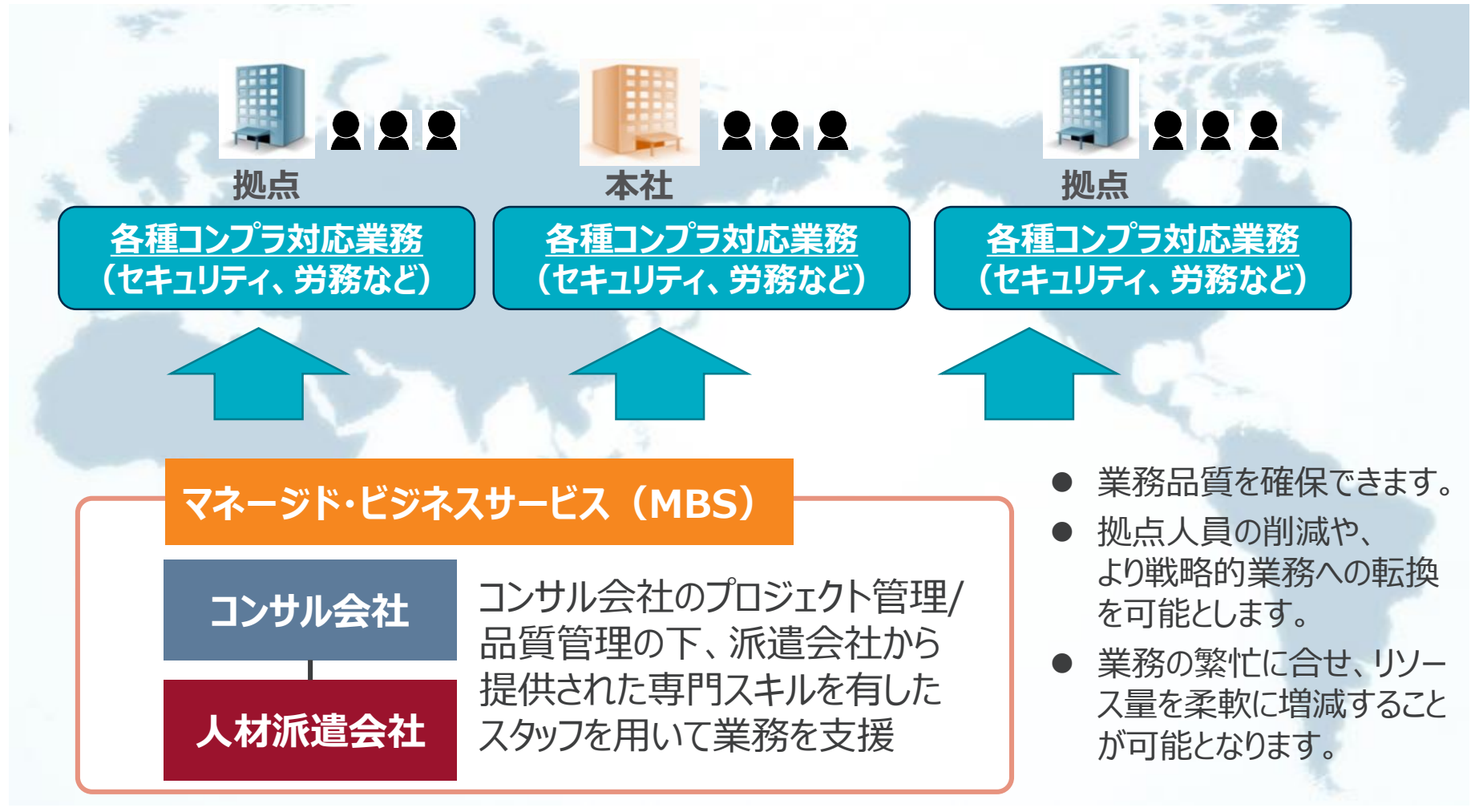
各国法規制情報を継続的に収集・更新を行い、各拠点への権限移譲範囲を基にした「グローバルの標準コントロール」の提示により、グループ会社のガバナンス体制強化を可能とします。



ご参考：多様かつ柔軟な人材確保の体制構築



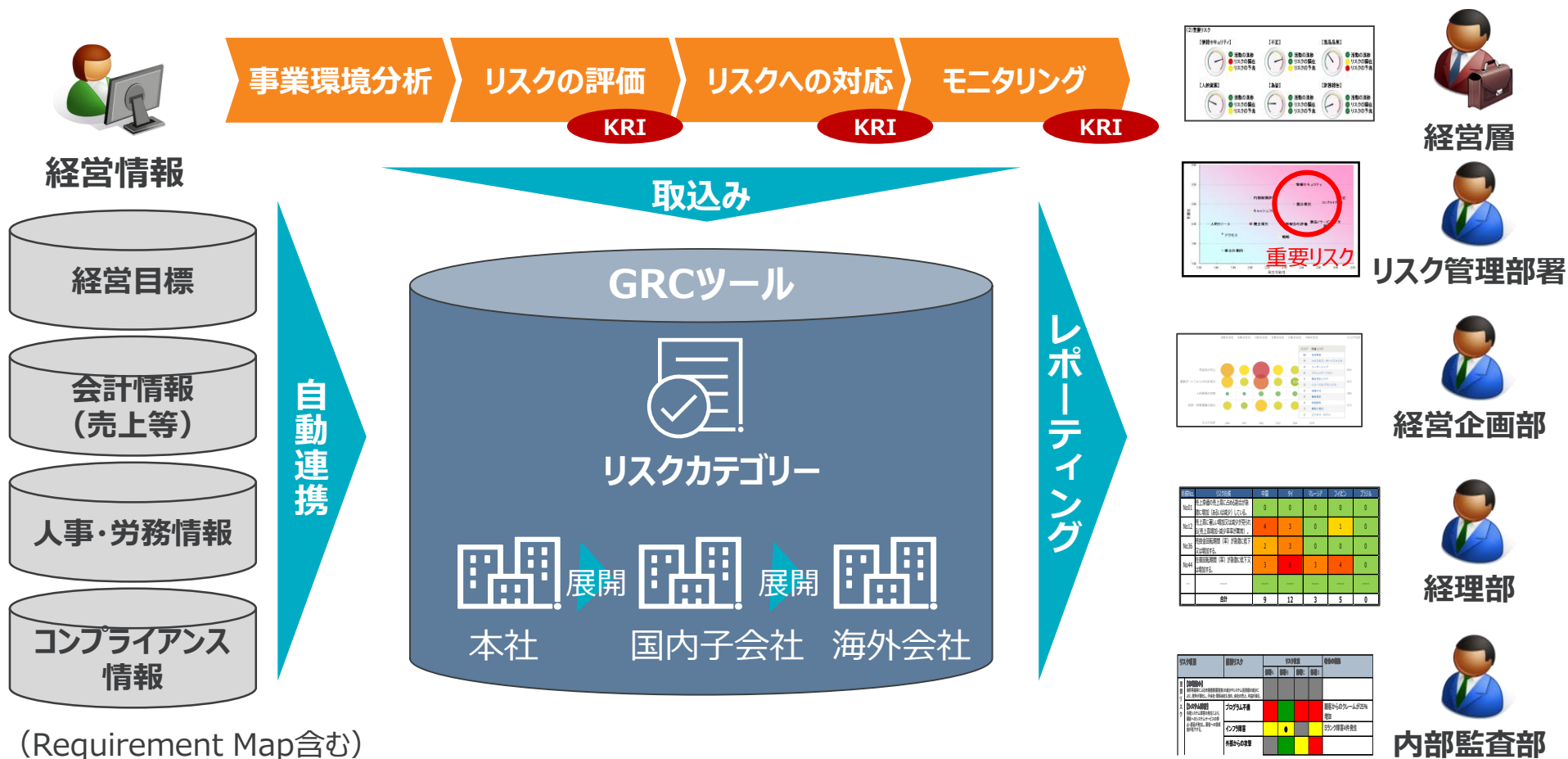
現在の拠点人員で新しいコンプライアンス要請に対応するには限界が生じていますが、専門スキルを有した人材を派遣することで、監督と指示の負荷を軽減させ、ビジネスに専念できる環境を可能とします。



ご参考：コンプライアンス管理基盤の構築

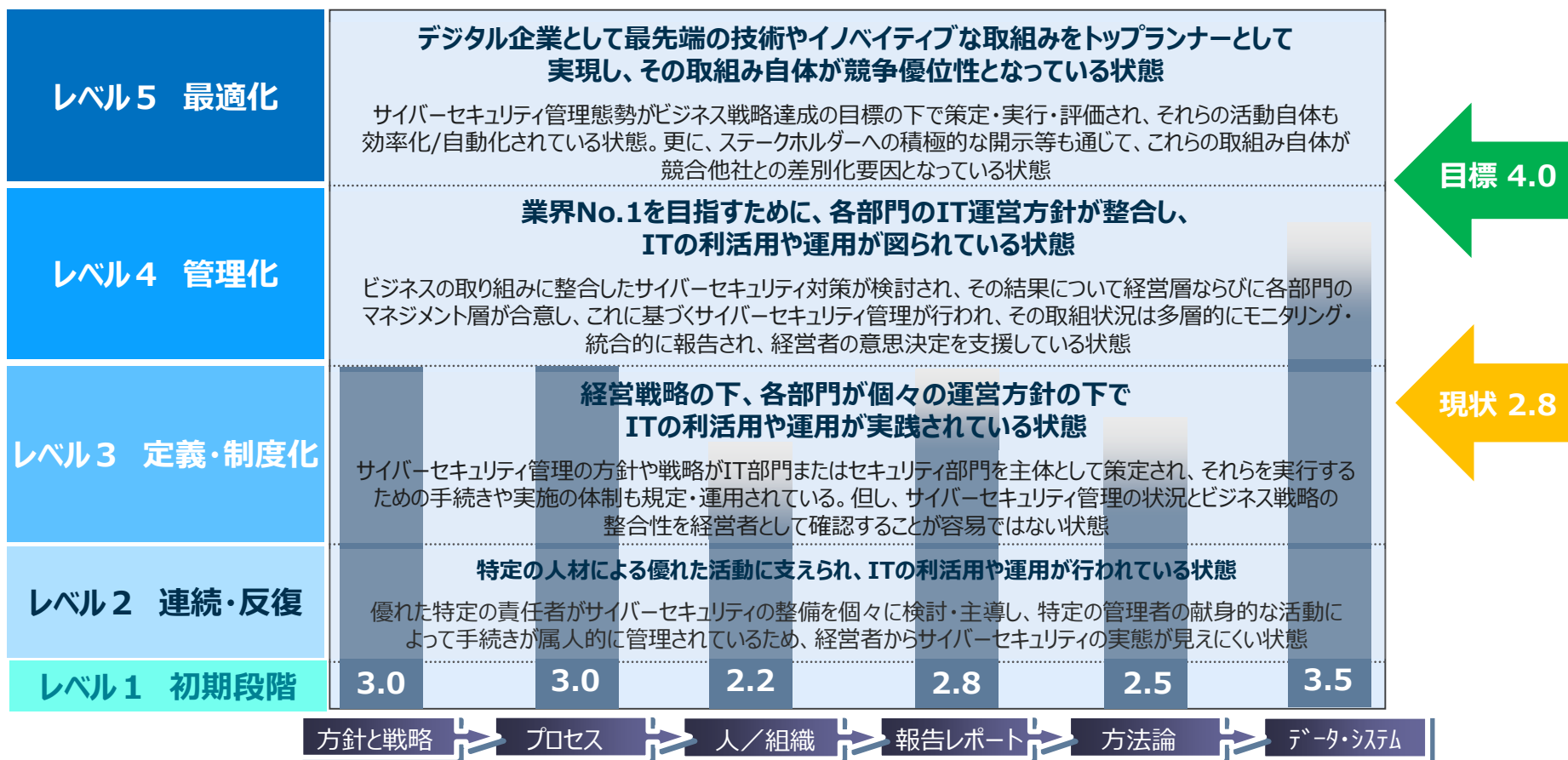


特定のコンプライアンス分野のみならず、様々なグループ経営に関するリスク情報と管理プロセスを統合し、グループガバナンスの有効性と効率性を確保する取組を可能とします。



ご参考：サイバーセキュリティリスク対応状況を評価・対処する（事例）

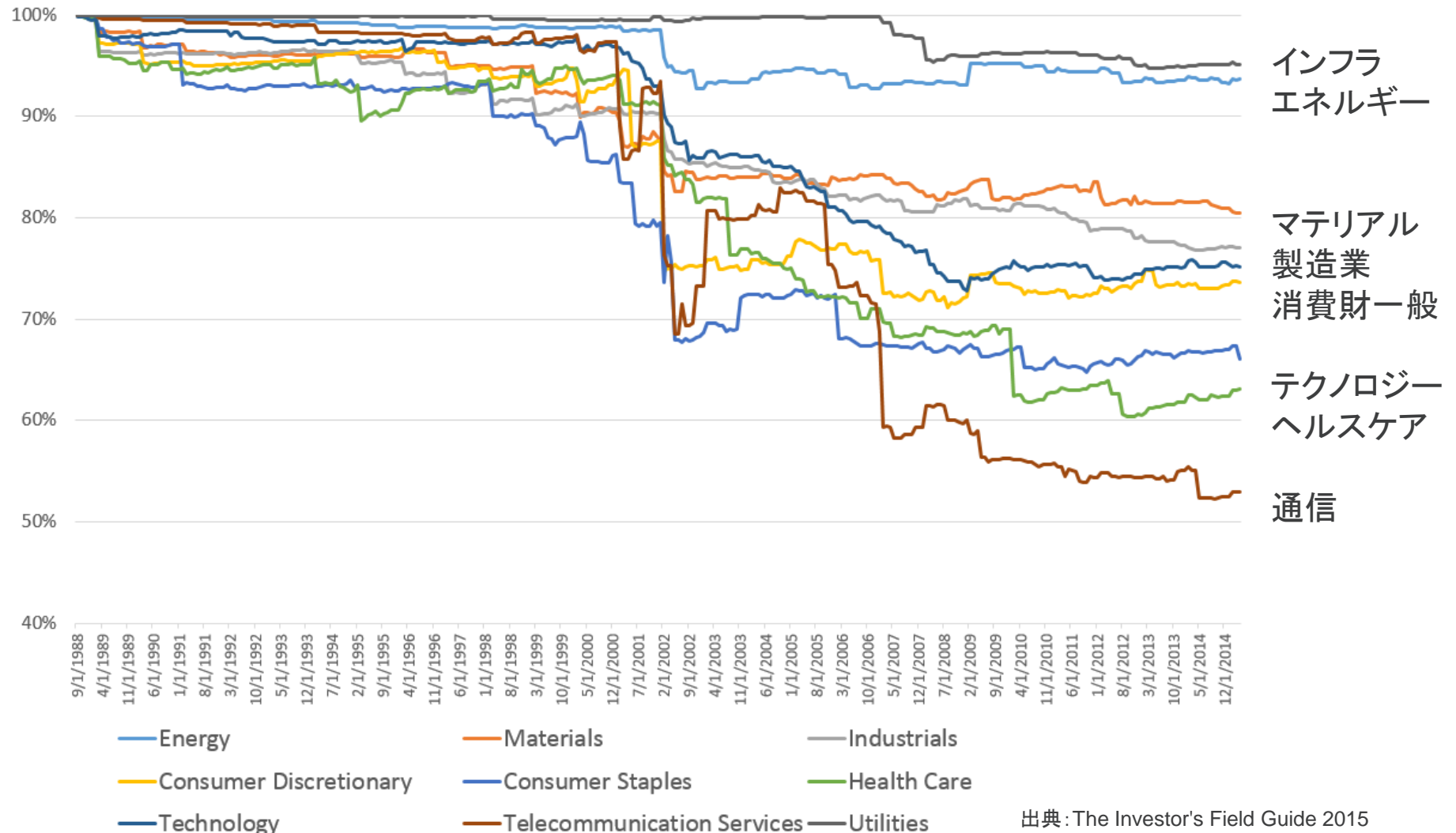
背景： サイバーセキュリティリスクには、NISTのフレームワーク等を活用して対応してきたものの、デジタル戦略が推進され、サイバー攻撃が多様化する中、サイバーセキュリティ管理態勢が維持できるかをリスク対応能力成熟度を使って評価した。



5. 人材トランスフォーメーションリスク

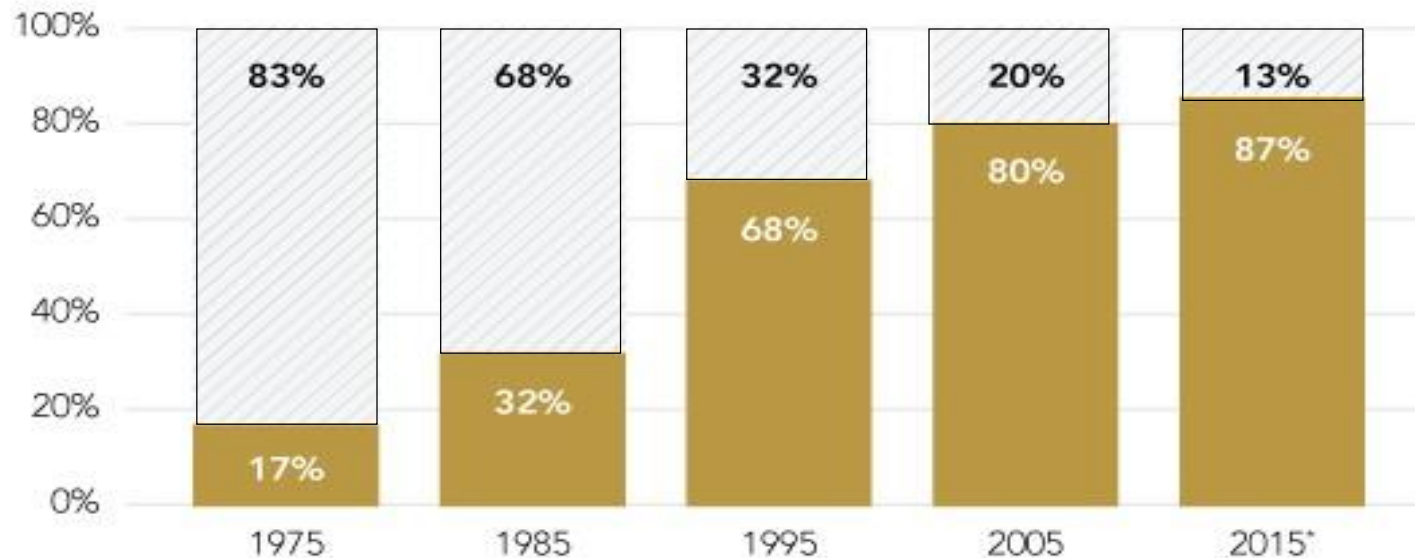
有形固定資産の総資産に占める割合が低下（米国1988～2014）

つまり、“目に見えない資産”が増加している ⇒ 如何にマネージするか



市場価値の構成要素 ～ S&P500 市場価値の構成要素～

Components of S&P 500 market value



有形資産（物的
および財務資産）

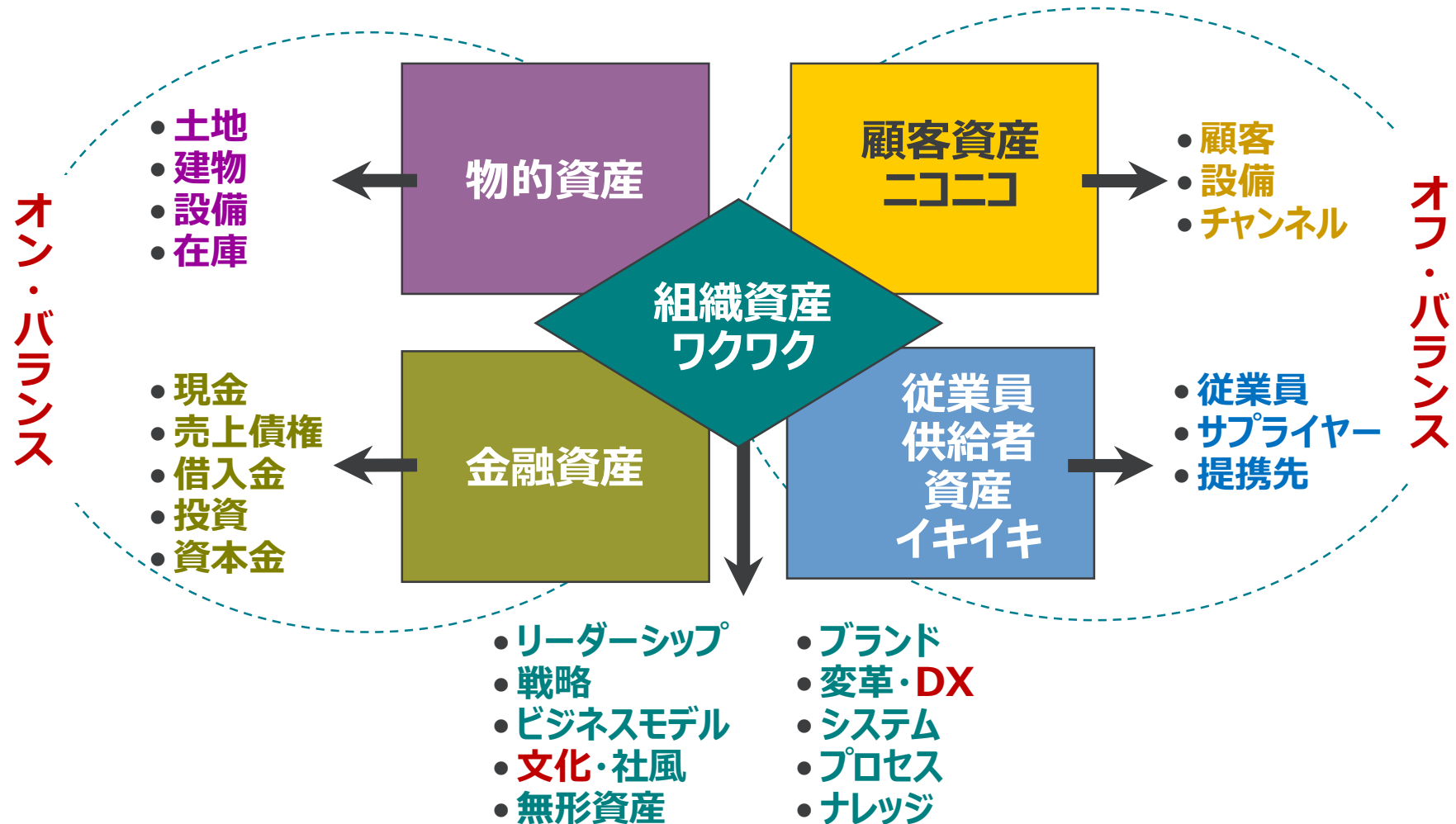


無形資産（組織資産等）

注：物的及び財務的資産（淡色）と、その他の要因（濃色）によって表される市場価値
出典：IIRC「統合報告に関するディスカッション・ペーパー」および、OCEAN TOMO, LLC

企業価値の源泉 ～バリューダイナミクス～

価値を生み出す資産は急速に変化している

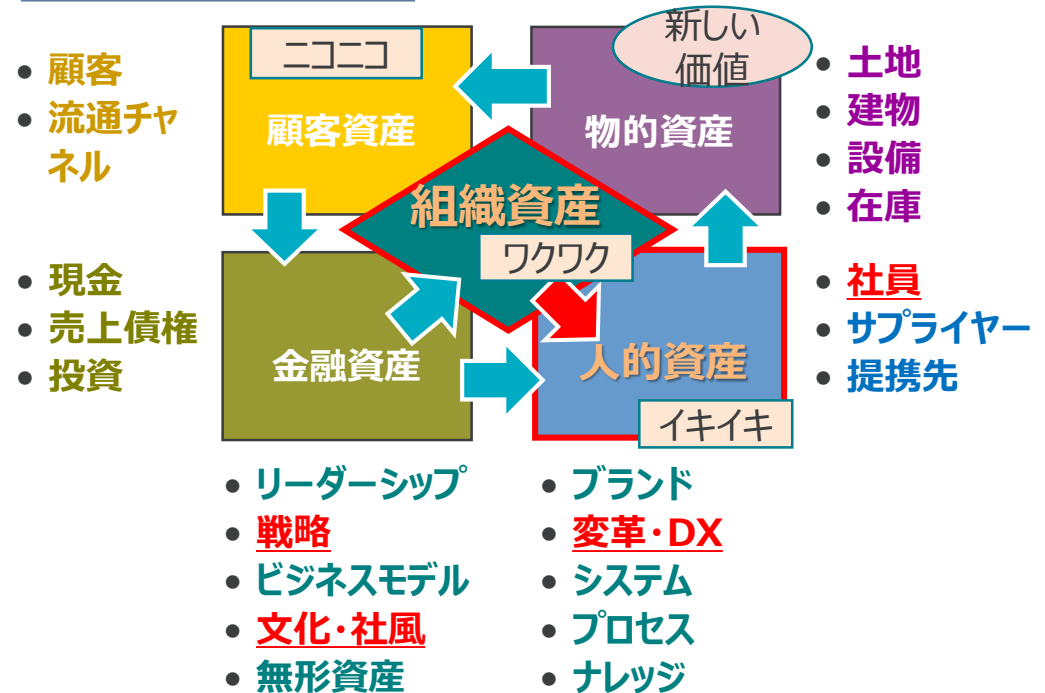




着眼点

- 一般に日本企業では退職率が低く、**良好な「安心基盤」**貴重な組織資産
- 更なる成長（新規事業等）には、企業文化や戦略に共感し、自発的に「イキイキ」行動するための組織資産としての「**ワクワク**」要素を常に新たにする工夫が必要
- 価値創造サイクルで、組織が「**ワクワク**」することにより社員が「**イキイキ**」し、その結果、新しい価値を生み出すことによりお客様の「**ニコニコ**」につながる。

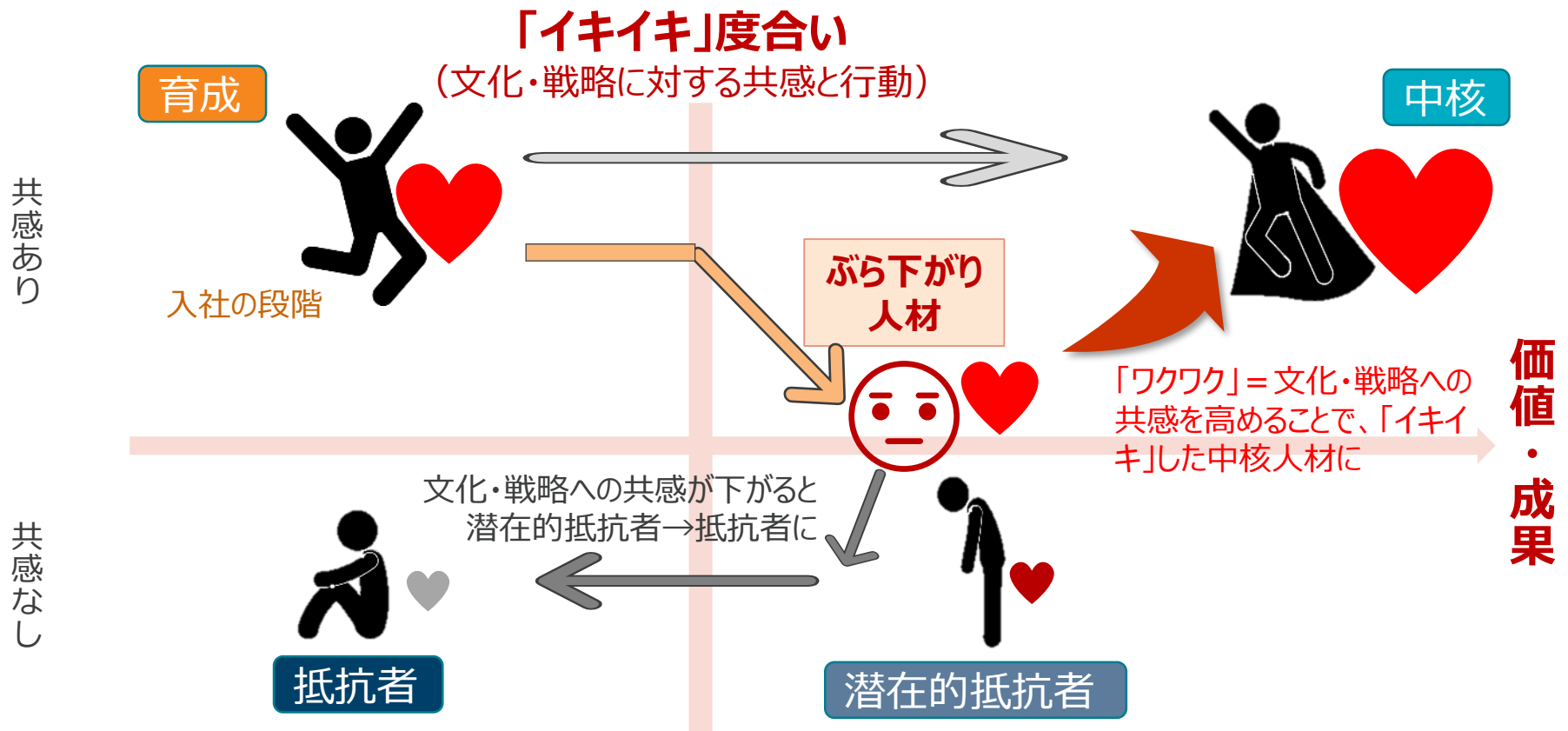
企業価値創造サイクル



価値創造のエンジンとしての人的資産

人的資産の「イキイキ」は、価値創造の重要なエンジン

- 人材の「イキイキ度合い」が低下すると、潜在的抵抗者・抵抗者となるリスクが高まる。
- 社員は高い期待をもって入社しますが、それに反する結果や評価が重なると、モチベーションが低下、その背景にある複合的な要素分析が重要です。



ご参考：人材トランスフォーメーションの成功要因

変革を成功させる5つの領域として、社員体験（EX）を重視

- 中長期的な制度改定、プログラムの継続的な改定
- 段階的な変革の深まり、エンゲージメントの向上をモニタリングするための仕組み作り

変革実現への5つの核となる領域



6. リスクと内部統制・ガバナンス

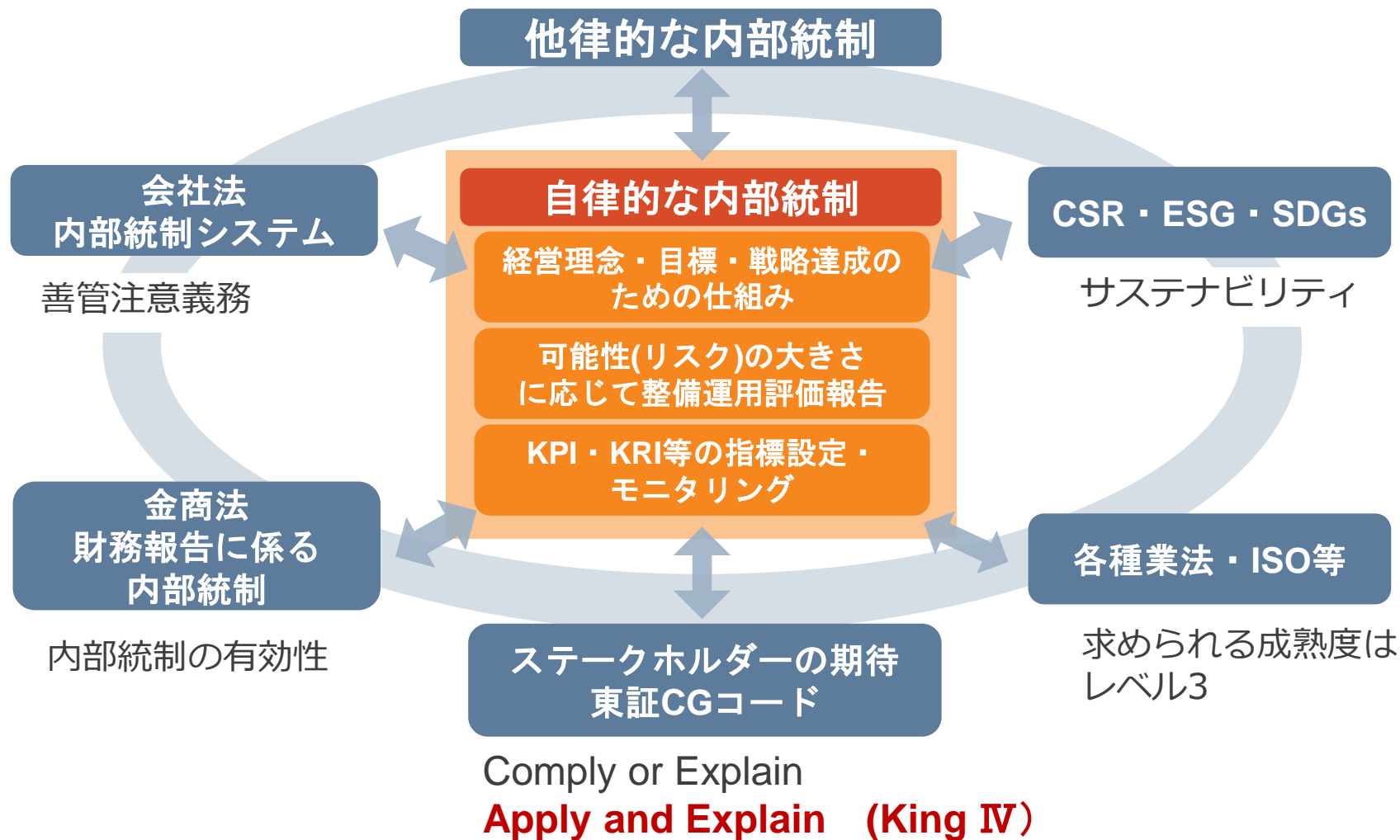
ガバナンス



不十分なガバナンスでは、戦略を誤り、リスクを見誤り、その結果、有効ではない内部統制により、やじろべえのバランスが崩れ、企業理念の達成が困難となります

リスクに偏らず、内部統制にも偏らず、中長期的にバランス感覚が求められます

自律的な内部統制と他律的な内部統制、どちらが大切な



*** 原則主義に則り、経営理念や方針に基づき、自らあるべき姿を念頭に構築・改善を継続する**

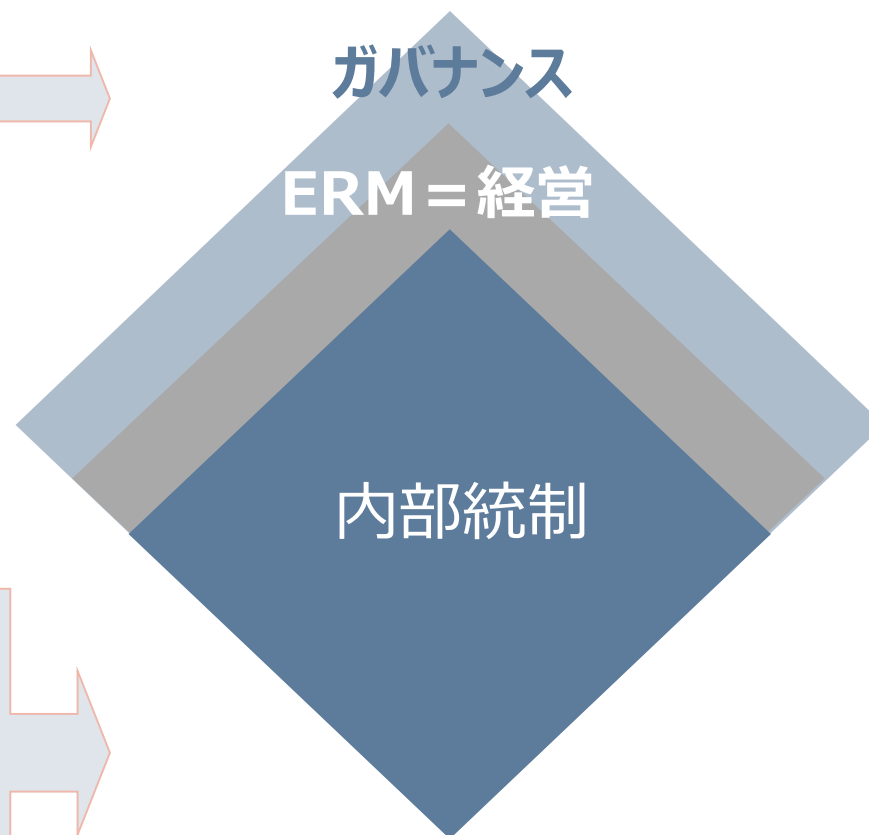
ご参考：ガバナンス・リスク・内部統制の関係をCOSOはどう整理したか

2013COSO内部統制は、ガバナンス・ERM・内部統制の関係を明示、三者の共通点はプロセス

内部統制はERMに包含され
ERMはガバナンスに包含されると言えども、
今や三者の境界は狭まっている

ERMフレームワークでは、
戦略目的を最上位とし、
機会と脅威の両面からリスクを特定し、
リスク選好（攻め）と許容度（守り）
を設定

内部統制とは、リスク許容度の範囲内に収まる
よう設計されたコントロール
5つのリスク対応：
活用*・受容・回避・転嫁共有・軽減の内、
最初の4つは戦略の課題であり、内部統制の
対象は許容範囲に収めるよう軽減



出典：2013及び2017COSO、
一部加工

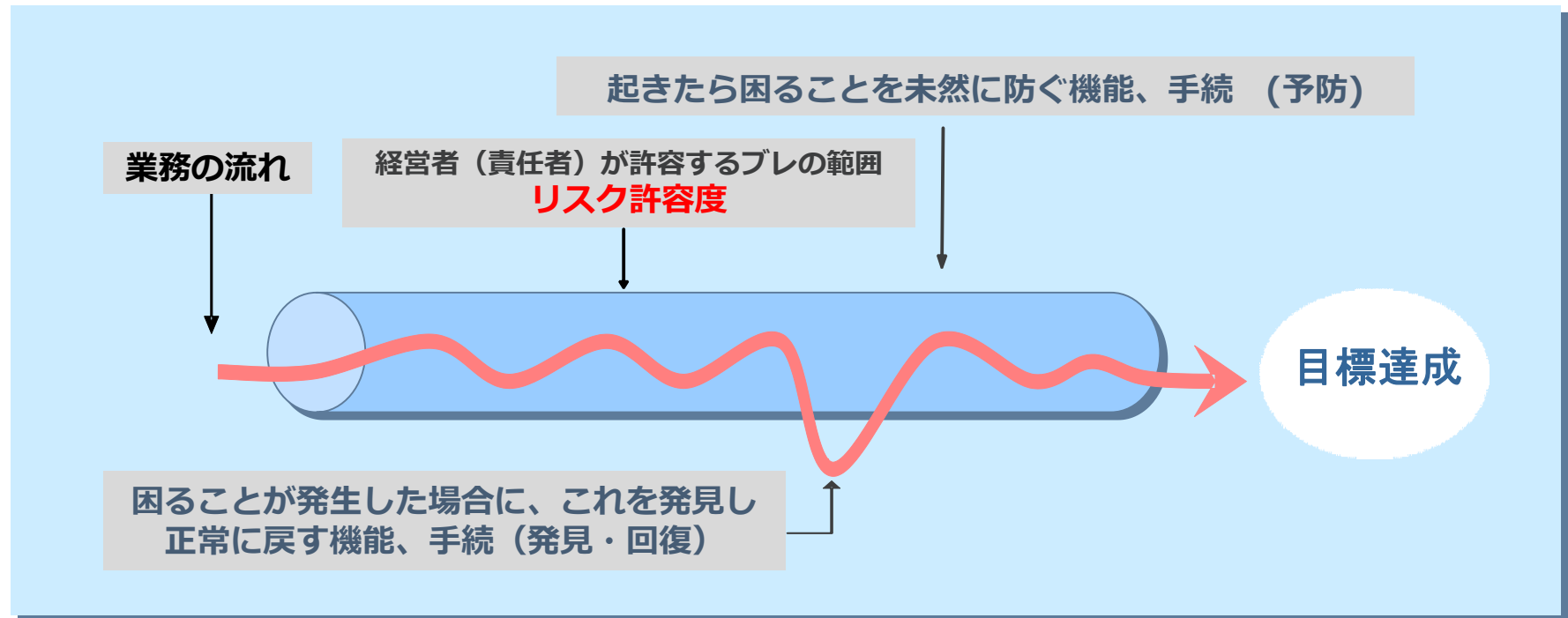
プロセスである限り、原則主義に則り、経営理念や方針に基づき、自らあるべき姿を念頭に構築すべきである

* 活用と受容の違いは、リスクプロファイルが受容では変わらないが、活用では変わる、つまり新規事業や大きなM&Aなどが活用の事例

業務レベルの内部統制～基本は予防と発見

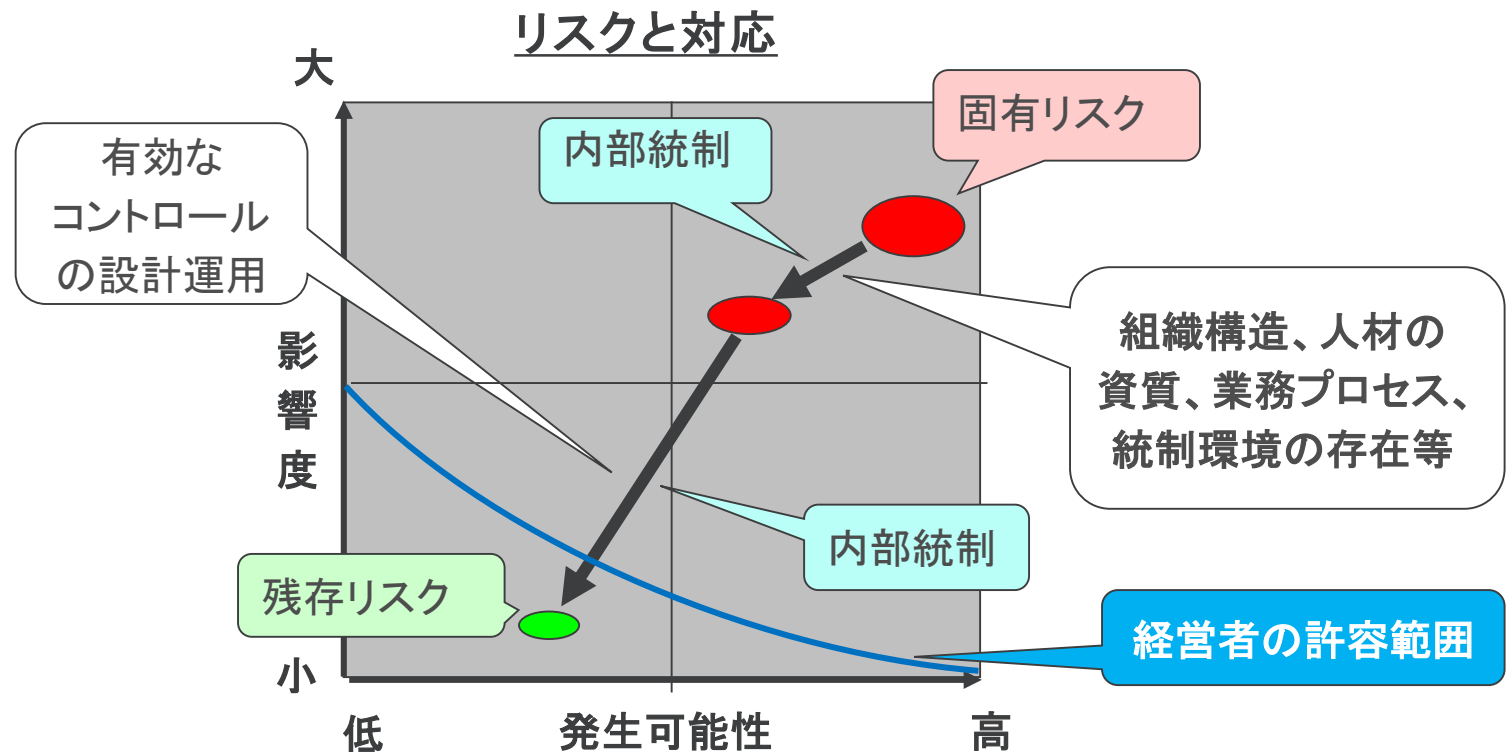
内部統制とは、目標を達成するためのPDCA活動を行う上で

- ◆ 起きたら困ることを起こさないための機能・手続（**予防**）
- ◆ 困ることを速やかに発見し正常に戻すための機能・手続（**発見・回復**）
をビルトインして、継続的に維持・改善する活動の総称



リスクと内部統制

～残存リスクと経営者の許容範囲

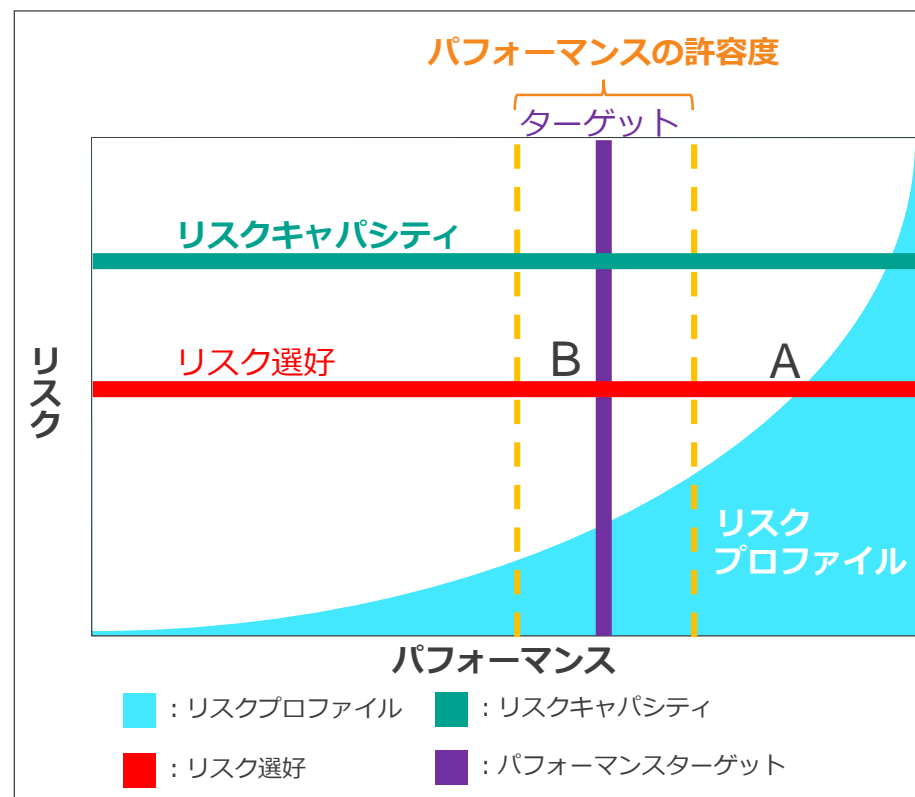


ご参考：リスク選好の決定

リスクプロファイル、事業環境、キャパシティ等様々な要因からリスク選好を決定

パフォーマンスとリスクの関係

- **リスクプロファイル**は、特定事業または全社戦略または目標に対するパフォーマンスレベルと累積リスクの総量で示される。
- リスク選好と**ターゲット**の交点Bは、リスク選好とリスクプロファイルの交点Aの左側にセットされる。合わせて**許容度**もセットする。
- リスク選好の設定は、**リスクキャパシティ**の範囲内に留めるべきだが、リスクキャパシティを超えた英断を求められることもある。
- リスク選好の緻密さを向上させるため、各種の**パラメータ**を設定する
 - **戦略パラメーター**
新製品の追及または回避、CAPEXによる投資、M&Aなど
 - **財務パラメーター**
最大限に許容可能な財務上のパフォーマンスとの差異、ROAまたはリスク調整後のROC、ROIC、ROE、格付など
 - **業務パラメーター**
環境規制要件、安全目標、品質目標、顧客集中度など



※各点のプロットは、定量的アプローチにも定性的アプローチも可能である。戦略又は事業目的に関して十分なデータを持っている場合、確率モデル、回帰分析などの定量的なアプローチが可能である。データが十分ではない場合や、事業目的がそれほど重要ではない場合には、インタビュー、ファシリテーション・ワークショップ、ベンチマーキングなどの定性的なアプローチが用いられる。

内部統制は不正を撲滅できるか

1. 会計不正の関与者と共謀・単独不正の状況

形態 \ 関与者	役員 + 管理職	非管理職	合計
共謀（外部 + 内部）	56 (外部17、内部39)	23	79 (61%)
単独	19	31	50 (39%)
合計	75 (58%)	54 (42%)	129 (100%)

出典：経営研究調査会研究資料第5号（日本公認会計士協会2018年6月26日）一部加工

2. 職業上の不正と濫用に関する国民への報告書(ACFE2018年度版より)

不正の手口：資産の不正流用89%、**汚職38%**、財務諸表不正10%

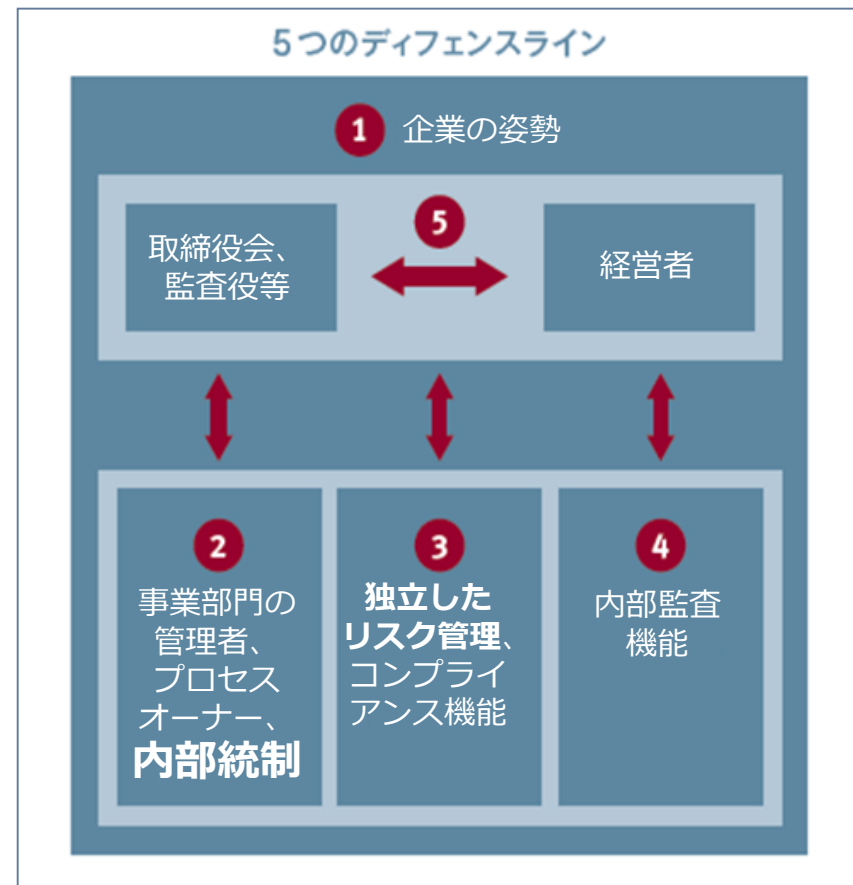
発見の手段：**通報40%**、内部監査15%、マネジメントレビュー13%、外部監査4%

不正関与者：従業員44%（5万ドル）、管理職34%（15万ドル）、**役員19%**(85万ドル)

5 線モデル(ディフェンスライン)で考える

—「企業の姿勢」の重視

- ◆ ガバナンス、リスク管理、内部統制が有効に機能するには「**企業の姿勢**」(Tone)が最重要。
- ◆ 「企業の姿勢」とは、経営トップ、中間層、現場の姿勢の**複合的姿勢**だが、激変する環境のもと、それぞれの姿勢は**同じではない**との前提に立つ。
- ◆ 企業の姿勢を組織の隅々まで反映させるには、先ず**経営層と管理者層の間でトーンを合わせる**事が大切
- ◆ トーンを合せるには、「**リスク・内部統制の共通言語**」を構築・浸透させることが必要不可欠。
- ◆ 「共通言語」とは、企業の姿勢・バリュー・理念、ERMの目的・方針・役割分担・リスク定義・許容度・評価・対応・報告等、ERMプロセスの総称



不正対応でのポイント：

トップの姿勢、悪い知らせが疎まれない“空気”、タイムリーなコミュニケーション、節度あるプレッシャーとインセンティブ、不正リスクマネジメントの本格導入とコントロールのビルトイン、KPI/KRIによるリアルタイムモニタリングによる牽制と発見、カルチャーの見直し（多様な価値観・目的・ベストプラクティスが共有され、風通しのよさや、倫理的行動が徹底される—以心伝心が実現できる—組織風土づくり）

ご参考：リスク監視・ディフェンスラインの失敗事例

最近の複数の第三者委員会調査報告書の分析結果について、リスク監視と5つのディフェンスラインから考える

第三者委員会報告書により指摘された不正会計の原因

1線：企業の姿勢	・ 上司の意向に逆らうことができないという企業風土 の下、目標達成のため不正な会計処理を実行
2線：事業部門	・ 当期における利益を最大化するために、 利益の先取りや損失・費用の計上先送り などを行わざるを得ないほどのプレッシャーを受けていた。
3線：財務経理部門	・ 財務経理部は 会計処理の適切性をチェックする役割 を果たすことなく、むしろ不正に関与
4線：内部監査	・ 内部監査部は経営トップが所管し、独立性を欠き、リスクアプローチが取られていなかった。
5線：経営者と取締役会	・ 経営トップらの関与 等に基づき不正な会計処理が継続された。 ・ 損失の発生が見込まれる案件が存在したにもかかわらず、 取締役会で報告されていなかった 。 ・ 監査役等は、不正な会計処理が行われている事実を認識しても、必要な対応を取らなかった。

我が国コーポレートガバナンスコード（改訂版）における「攻めと守り」のリスク

- 取締役会の役割として、「**経営陣幹部による適切なリスクテイクを支える環境整備**を行うこと、独立客観的立場から経営陣・取締役の実効性の高い監督を行うこと」（基本原則4）
- 「取締役会は、**内部統制やリスク管理体制を適切に整備**すべきである。」（原則4－3(3)）
- 「**コンプライアンスや財務報告に係る内部統制や先を見越したリスク管理体制の整備**は、適切なリスクテイクの裏付けとなるが、取締役会は、これらの体制の…の監督に重点を置くべきであり、個別コンプライアンスの審査に終始すべきではない」（補充原則4－3④）

CGコードのポイント：

- リスクテイクを支える環境整備、独立した立場からの**経営陣・取締役に対する実効性の高い監督、内部統制やリスク管理体制の適切な整備とその運用の有効性の監督、**を取締役会の役割とし、これは2010年から米国でスタートした**リスクオーバーサイト***そのもの。
- コンプライアンスなど、「**報われないリスク**」という守りを対象にしている一方で、「**先を見越したリスク管理体制**」など「**報われるリスク**」の攻めも含められている。

* SEC規則により、2010年から、株主総会招集通知にリスクマネジメントにおける取締役会の役割を記載するもので、攻めのリスクテイクと守りのリスク管理に関する取締役会、各委員会の役割を具体的に開示。

ご参考：リスク監視とガバナンス

世界金融危機を教訓に、取締役会にリスク監視の機能を義務付け、SECが開示を要請したもの、続けて、NACDがリスク監視の10原則を発表

取締役会に期待される機能と役割（全米取締役協会の10原則）

1

企業の成功要素を理解する

2

戦略に固有のリスクを評価する

3

リスク監視に係る取締役会、委員会の役割を定義

4

リスク管理や内部統制が適切か、提供される資源が適切か検討する

5

取締役会に提供されるリスク情報に関して、種類、報告様式を執行陣と合意する

6

取締役会と執行陣が建設的にリスクを協議する

7

社風とインセンティブに係るリスクをモニタリング

8

戦略、リスク、インセンティブへの準拠状況をモニタリング

9

何が次に来るのか、新たなリスクや派生するリスクに関して検討する

10

取締役会のリスク監視の目的が達成されているか、定期的に監視プロセスの実効性評価を行う

- 透明性transparencyがないところで、説明責任accountabilityは果たせない、という姿勢
- 意思決定において透明性を図り、説明責任を果たすには、取締役会にて議論を尽くす
- 取締役の候補者の透明性ある選定プロセスと、報酬インセンティブに対する考え方が大切

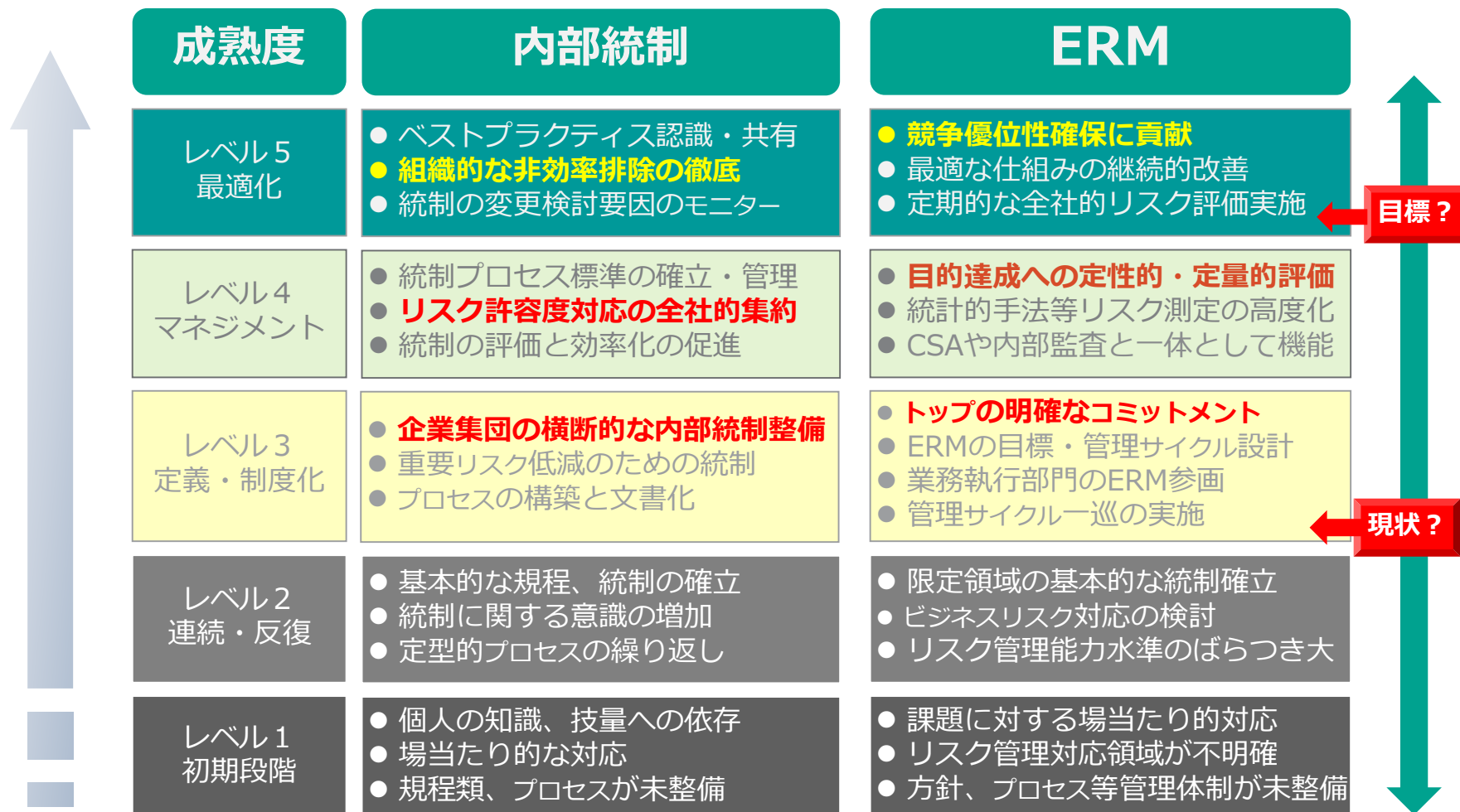
ご参考：ガバナンスの高度化～Chain of Accountability

アシュアランスマップにより、責任連鎖を可視化し、合理的保証の輪を拡げる。
誰が、どのリスクを、どこまで管理できているか

	経営者 による レビュー	各種委員会	取締役会	監査役等 (事務局含)	外部 監査人	内部 監査人	ISO 評価者	現在のア シュアラン スレベル	将来のア シュアラン スレベル
財務報告									
内部統制									
資金調達									
投資									
環境									
法務コンプライアンス									
IT									
リスクマネジメント									
不正									

高アシュアランス
 中アシュアランス
 低アシュアランス
 アシュアランスがあるべき分野
 該当なし

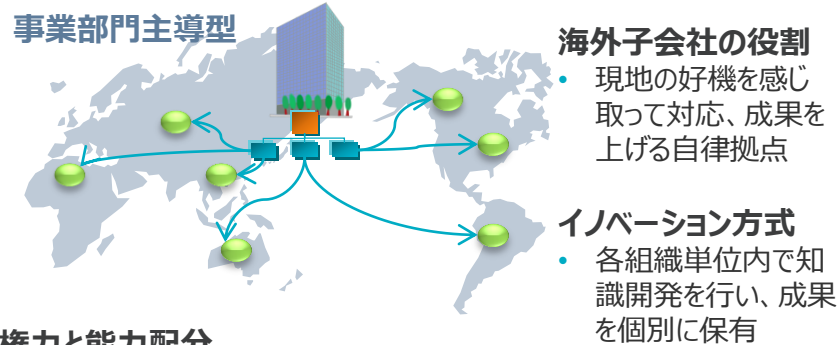
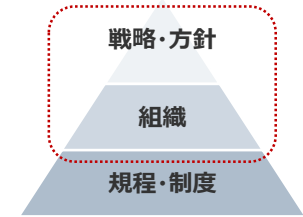
ガバナンスの高度化～経営インフラの成熟度を高める



(例えば、会社法内部統制や金商法JSOXはレベル3)

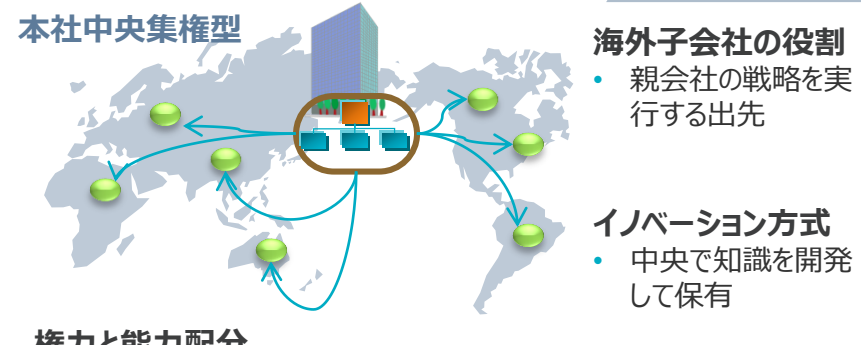
ご参考：グローバルガバナンスの方向性

グローバルガバナンス強化にあたって、グローバル経営モデルを明確にすることも有用です。



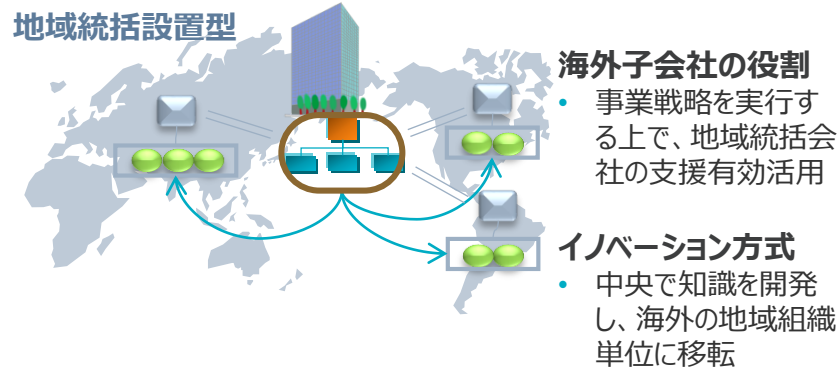
権力と能力配分

- 各事業部門に分散
- 海外子会社は自立している、または各事業部門が管理



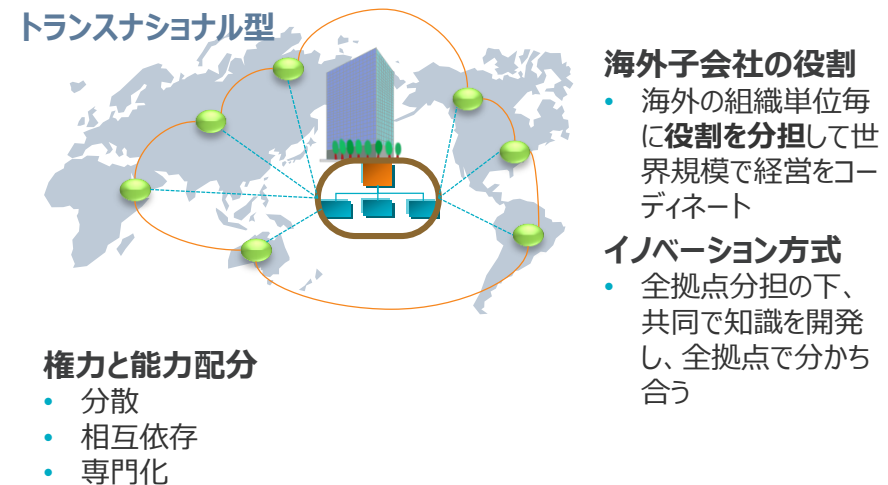
権力と能力配分

- グローバル本社に集中
- グローバル展開
- 規模の経済重視



権力と能力配分

- 能力の中核部はグローバル本社に集中させ、他は地域統括会社に分散



権力と能力配分

- 分散
- 相互依存
- 専門化

まとめ

ご参考：記述情報の改正（内閣府令、2019年1月31日）

記載項目	新たに要請される記載事項	COSOERM
(1)経営方針、経営環境及び対処すべき課題等	①事業内容と関連した経営方針・戦略・事業環境 ②経営方針・戦略と関連して対処すべき事業上及び財務上の課題、対処方針	構成要素 1、2
(2)事業等のリスク	①主要なリスクが顕在化した場合に経営成績等に与える影響 ②主要なリスクが顕在化する可能性 ③主要なリスクへの対応策 ④主要なリスクに関する経営方針・経営戦略と関連した記載 ⑤事業活動の継続に関する重要事象の内容、分析・検討内容、解消・改善するための対応策	構成要素 2、3、4
(3)財政状態、経営成績及びキャッシュ・フローの状況の分析	資金調達方法・状況並びに資金の主要な用途を含む資金需要の動向	構成要素 2、3

今後、事業等のリスク情報の開示は、経営方針・戦略・事業環境と関連させたリスクの特定評価結果の開示が求められ、全社的リスク管理の方針明確化と組織内の一層の連携が必要です。価値創造ストーリーの中で、特定した重要なリスクに対し、KAMの候補項目も含め、内部統制の有効性を確保しておく必要があります。

ご参考：KAMの導入：財務諸表監査における「監査上の主要な検討事項(2019年度以降)」

概要	2021年3月期決算より、財務諸表監査報告書に「監査上の主要な検討事項」（監査人が当年度の財務諸表の監査において特に重要であると判断した事項）の内容、「監査上の主要な検討事項」と決定した理由及び監査における対応が記載されます（2020年3月期から早期適用可能）。
目的	財務諸表監査プロセスの透明性向上を通じた以下の事項 <ul style="list-style-type: none"> ・財務諸表監査の信頼性向上 ・財務諸表利用者と経営者との対話の促進 ・監査人と経営者、監査役等とのコミュニケーション促進によるコーポレート・ガバナンスの強化
主な検討事項	監査人が監査の過程で監査役等と協議した以下の事項等 <ul style="list-style-type: none"> ・特別な検討を必要とするリスクが識別された事項、又は重要な虚偽表示のリスクが高いと評価された事項 ・見積りの不確実性が高いと識別された事項を含め、経営者の重要な判断を伴う事項に対する監査人の判断の程度 ・当年度において発生した重要な事象又は取引が監査に与える影響
求められる対応	自社の事業上のリスクと、当該リスクを考慮した財務報告リスクを把握した上で、「監査上の主要な検討事項」について監査人と協議することが求められます。



KAMの議論においては、特に機微情報の取扱いも含め、執行陣、監査役等、外部監査人の三者でのコミュニケーションが重要。有報と会社法事業報告の一体化や開示時期は企業側の姿勢の問題でもある。

次世代のリスクマネジメントを目指して

欧米では、リスクテイクのためにリスク管理を行い、過度なリスクテイクを回避するために、ガバナンスを強化している。

日本では、リスク回避のためにリスク管理を行い、リスクテイクのためにガバナンスを強化している。リスクテイクを推進するには、ガバナンス、内部統制と一体となったリスク管理の高度化が不可欠です。

1. 企業の姿勢や社風を見つめ、風通しのいい“空気”を保つ
2. 攻めと守り、リスクの両面からリスクを見極める
3. ガバナンス改革とERM・内部統制の高度化は一体となって推進する
4. 原則主義の徹底～JSOXなどリスク・コンプライアンスの形骸化に対応する
5. ERMの考え方を活用し、ESG/SDG sを含め、グローバル組織横断的な説明責任連鎖の強化、合理的保証を確保し、変化に適応し企業理念・戦略の実現を中長期的に、より確実なものとする。

リスク管理・内部統制で最も大切なのはトップの姿勢であり、社訓に基づき、自律的な仕組みを継続的に強化することで激変する変化に対処し、常に最終決断を迫られる“孤独”なトップの果敢な挑戦を支える次世代のリスクマネジメントの構築を目指すことが求められています。



Face the Future with Confidence